BIDANG ILMU : REKAYASA

LAPORAN PENELITIAN HIBAH BERSAING
(Tahun ke-1)

REKAYASA SOFTWARE ANTIVIRUS JENIS WORM SEBAGAI ALTERNATIF SOLUSI PENANGGULANGAN SERANGAN VIRUS WORM KOMPUTER

Oleh :

Heribertus Yulianton, S.Si, M.Cs
Arif Jananto, S.Kom, M.Cs
R. Soelistijadi, S.Sos, M.Kom

Dibiayai oleh Koordinasi Perguruan Tinggi Swasta Wilayah VI, Kementerian Pendidikan dan Kebudayaan, sesuai dengan Surat Perjanjian Pelaksanaan Hibah Penelitian Nomor : 023/006.2/PP/SP/2012 tanggal 24 Februari 2012

UNIVERSITAS STIKUBANK SEMARANG
FAKULTAS TEKNOLOGI INFORMASI

November 2012

HALAMAN PENGESAHAN

1. Judul Peneltian : Rekayasa Software Antivirus Jenis Worm Sebagai Alternatif Solusi Penanggulangan Serangan Virus Worm Komputer

2. Ketua Peneliti :

a. Nama Lengkap	: Heribertus Yulianton, S.Si, M.Cs
b. Jenis Kelamin	: Laki-Laki
c. NIP	: YS.2.98.11.015
d. Jabatan Struktural	: Kepala P2ICT
e. Jabatan Fungsional	: Penata /Asisten Ahli/III B
f. Fakultas/ Jurusan	: Teknologi Informasi /Teknik Informatika
g. Pusat Peneltian	: LPPM Universitas Stikubank (UNISBANK
h. Alamat	:Jl. Trilomba Juang No.1 Semarang
i. Telepon/Faksimail/E-mail	:(024)8311688/ Fax (024)8443240 info@unsibank.ac.id
j. Alamat Rumah	:Jl. Sadewo I No 05 -semarang
k. Telepon / Email	: 08122516688/heri@unsibank.ac.id

3. Jangka waktu Penelitian : 2 Tahun

4. Pembiayaan

a. Jumlah Biaya Tahun ke-1	: Rp. 29.707.500
- Biaya Tahun ke-1 diajukan ke Institusi lain	: Rp. -

Semarang, 20 November 2012

Mengetahui,
Dekan Fakultas Teknologi Informasi

(Dwi Agus Diartono, M.Kom)
NIY: Y.2.90.03.054

Ketua Tim Pengusul,

(Heribertus Yulianton, S.Si, M.Cs)
NIY: YS.2.98.11.015

Mengetahui,
Kepala LPPM UNISBANK,

(Dr. Dra. Lie Liana, M.MSi)
NIY: Y.2.92.07.085

Abstraksi

Ancaman terhadap virus jenis worm saat ini sangat banyak dan meresahkan para pengguna komputer personal maupun mobile, karena talah banyak yang terjangkiti. Meskipun terdapat berbagai macam jenis antivirus telah beredar dipasaran, namun jenis antivirus yang dikhususkan untuk menanggulangi virus jenis worm 32/cyrax dan gratis sangatlah terbatas. Untuk itu penelitian ini bertujuan membuat sebuah software antivirus jenis worm 32/cyrax yang berfungsi untuk menanggulangi jenis ancaman worm tersebut yang tersedia gratis untuk masyarakat.

Metode yang digunakan dalam penelitian ini adalah *action research*, dengan model pengembangan sistem informasi model *prototyping*. Metode ini digunakan karena pengembangan yang dilakukan dimulai dari tahapan identifikasi, analisis, desain, implementasi dan pengujian hasil akan dilakukan secara siklus berulang untuk melengkapi temuan-temuan dari tahapan yang dirasakan kurang sempurna. Luaran dari penelitian ini adalah berupa software aplikasi antivirus yang dapat mendeteksi adanya Worm W32/Cyrax dan sekaligus dapat menghapus atau menghilangkannya dari data atau file yang terjangkit.

Kata Kunci : Virus, Worm, W32/Cyrax, Antivirus.

KATAPENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa bahwa penelitian Hibah Bersaing pada tahun pertama ini telah selesai dilaksanakan dengan baik. Penelitian ini bermaksud untuk membuat perangkat lunak antivirus jenis worm W32/Cyrax yang nantinya dapat dimanfaatkan bagi masyarakat secara luas. Harapannya bahwa hasil penelitian ini bisa dapat digunakan untuk menangulangi serangan virus jenis worm terutama W32/cyrax, sehingga nantinya masyarakat tidak lagi terganggu terhadap jenis serangan virus worm tersebut dan dapat menggunakan perangkat komputer dengan aman tanpa takut kehilangan atau kerusakan data.

Penyusun ucapkan terimakasih kepada semua pihak yang telah membantu terlaksananya penelitian ini, terutama DIKTI yang telah mendanai dan teman-teman kampus yang memberikan masukan. Penelitian ini masih perlu terus dikembangkan, untuk itu saran dan kritik dari pembaca agar penelitian ini dapat disempurnakan. Dan dapat dijadikan acuan bagi penelitian-penelitian lanjutan yang lebih memberikan manfaat bagi para pembaca khususnya dan bagi kemakmuran masyarakat Indonesia.

Semarang, November 2012

Penyusun

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Resiko kerugian pada pemakaian perangkat teknologi informasi terutama komputer, dapat timbul sewaktu-waktu dengan cara tidak sengaja, maupun disengaja. Resiko kerugian yang tidak disengaja, dikarenakan tidak berfungsinya sistem akibat seperti kelalaian operasi, pemeliharaan (*maintenance*) yang kurang memadai, perangkat yang usang, atau karena faktor alam seperti bencana alam dan cuaca. Sedangkan resiko kerugian yang disengaja merupakan bagian bentuk kejahatan dalam pemakaian teknologi informasi, termasuk diantaranya kejahatan yang dilakukan melalui serangan (*attack*) berupa serangan virus komputer dan atau melalui jaringan internet, sehingga sering disebut sebagai *cybercrime*.

Ancaman virus komputer merupakan momok bagi para pengguna komputer, apalagi dengan adanya jaringan komunikasi global (internet), maka virus akan lebih mudah dan leluasa menyerang dan menyebar luas melalui akses internet. Pemakaian aplikasi jejaring sosial seperti facebook, twiter, dan e-mail merupakan jalur yang paling rentan akan datangnya serangan virus. Kerugian terhadap serangan dan penyeberan virus computer telah banyak menghabiskan biaya, baik biaya yang diakibatkan karena telah terjadi serangan virus tersebut, atau besarnya biaya untuk melakukan pencegahan dan penanggulangannya.

Bahkan perusahaan antivirus terbesar symantec corp., merilis informasi terbaru mengenai beberapa ancaman yang termasuk kedalam kategori kejahatan komputer (*Computer-Crime*) yang terjadi selama tahun 2009. Menginformasikan dengan kehadiran situs *social networking* (facebook, twitter, dan sejenisnya), sebenarnya ada banyak bahaya yang mengancam, atau bahkan mungkin sistem kita sudah menjadi korban, namun terkadang tidak disadari. (http://ekofiles.darmajaya.ac.id/index.php/info-terbaru/58-symantec, 2009)

Bahkan ancaman virus computer jenis worm, saat ini telah banyak menyerang tidak hanya pada computer, tetapi juga perangkat handphone. Virus ponsel adalah sejenis virus komputer yang menyebabkan aplikasi ataupun fitur ponsel tidak dapat digunakan semestinya. Kecanggihan ponsel hampir mendekati teknologi komputer. Ponsel juga telah menggunakan sistem operasi terbuka sehingga aplikasi buatan pihak ketiga bisa melengkapi kecanggihan dari fungsi standar pabrikan. Sistem operasi terbuka inilah yang akhirnya menjadi celah bagi masuknya program jahat seperti virus, worm, dan juga Trojan horse. Biasanya virus disamarkan dalam bentuk yang menarik seperti game ataupun gambar. Supaya lebih menarik lagi, permainan ataupun gambar tersebut diselipkan kata-kata yang vulgar (http://www.forum-bonecommunity.com/ 2009).

Virus ponsel menyebar melalui media seperti: bluetooth, infrared, Wi-Fi, dan kabel data serta internet. Ponsel semakin rawan dengan infeksi virus dan ini dikarenakan handphone sudah menjadi peranti canggih untuk komunikasi data. Walaupun pemakaian handphone yang mampu mengirim dan menerima file

(smartphone) masih terbatas, namun hal ini harus tetap diwaspadai pada masa-masa yang akan datang. Bagi perusahaan yang karyawannya banyak menggunakan PDA phone atau smartphone, maka ancaman virus bagi jaringan perusahaan tersebut bisa semakin meningkat. Untuk itu dibutuhkan keamanan yang baik pada lingkungan perusahaan tersebut. Penyebaran virus ponsel hampir tidak bisa dikenali, berbagai cara telah dilakukan dalam menginfeksi ponsel. Pengguna ponsel bermemori besar tentunya kerap melakukan transfer data dari kartu memori ponsel ke komputer. Pengguna pun harus berhati-hati melakukannya. Trend Micro, sebuah perusahaan antivirus asal Amerika Serikat mengumumkan keberadaan virus ponsel yang mampu menginfeksi komputer. Trend Micro mengungkap bahwa telah muncul virus yang dinamai Symbos_cardtrp.A Menurut peneliti di Trend Micro, virus tersebut awalnya beredar di ponsel berplatform Symbian Seri 60. Namun saat ini telah berkembang dan memiliki potensi untuk menyebar ke komputer yang beroperasi dengan sistem Microsoft Windows.

Banyak antivirus yang sekarang ini telah beredar dipasaran baik yang berbayar maupun yang gratisan, yang terkenal seperti Antivir personal dan provesional, AVG antivirus, Kaspersky, avast, anvast, dan masih banyak lagi yang lainnya. Namun begitu karena antivirus tersebut sifatnya yang general, yaitu digunakan untuk melakukan deteksi (*scanning*) berbagai macam virus yang jumlahnya bisa hingga ribuan, sehingga terkadang pada jenis virus tertentu seperti worm W32/Cyrax tidak dapat terdeteksi.

Dari hasil laporan penelitian yang dilakukan *Computer Economics* pada tahun 2006, menyatakan bahwa 99 persen perusahaan telah menggunakan antivirus, namun 76 persen di antara mereka mengakui terinfeksi virus. Sedangkan menurut hasil survey cisco (cisco.com) selama januari sampai dengan oktober 2007, kategori ancaman dan lubang keamanan (*vulnerability*) keamanan computer terbanyak adalah memori ”dibanjiri” dengan banyaknya lalulintas data (*Buffer Overflow*) , disusul penolakan layanan (*Denial of Service*), Perubahan kode eksekusi (*Arbitrary Code Eecution),* peningkatan otoritas (*privilage escalation*), dan terkecil adalah *symbolic link*. Sedangkan worm dan trojan pada tahun sebelumnya berada pada urutan bawah. Ini artinya diprediksi bahwa worm dan trojan pada periode yang akan datang akan menjadi ancaman yang peringkatnya terus meningkat. (http://research.indocisc.com/, 2006)

Menurut lembaga riset Gartner, pada tahun 2006, penduduk Amerika menderita kerugian finansial sebesar USD2.8 miliar akibat phishing yang menyebabkan organisasi "Rock Phish" menerima lebih dari USD100 juta. Sementara itu, volume spam Asia meningkat. Sepertiga dari spam non-English berasal dari Cina. Spam yang berhubungan dengan komersial dan financial masih tetap paling populer. Spam yang menggunakan bahasa Inggris meningkat 19% di Q1. Bahasa Jepang (58%) dan Cina (33%) adalah grup terbesar spam yang tidak menggunakan bahasa Inggris yang mengambil alih posisi bahasa Rusia dan Spanyol dalam mendominasi spam non bahasa Inggris tahun lalu. Bahasa Korea juga masuk dalam peringkat 10 besar bahasa non Inggris banyak dipakai untuk

spam. Alasan spam menggunakan bahasa-bahasa di Asia tersebut terus meningkat sebagian besar karena kini Eropa dan Amerika telah memiliki peraturan yang ketat terhadap masalah spam ini.(http://www.ketok.com, 2007).

Di Indonesia sendiri virus jenis worm lokal mulai menunjukkan aktifitas yang cukup signifikan di awal era millenium. Karena begitu pesatnya penyebaran virus komputer dan berbagai jenis worm.komputer local yang beredar di Indonesia terutama pada akhir-akhir ini, ternyata menimbulkan dampak yang sangat meresahkan bagi para pengguna komputer. Sehubungan dengan hal tersebut maka perlu adanya suatu perhatian khusus terhadap penyebaran virus-virus atau worm-worm tersebut.

Salah satu contoh worm yang telah beredar dan menyebar di Indonesia adalah worm tipe W32/Cyrax. Tipe worm ini sangat menggangu sekali pada setiap aktifitas pemakaian computer karena Worm ini mampu bekerja tanpa interaksi user, bisa merusak sebuah data secara langsung atau menurunkan kinerja suatu system dengan *'mengikat'* sumberdaya system computer dan bahkan bisa mematikan sebuah jaringan. Ciri yang paling mudah dikenali bahwa sebuah computer terkena worm adalah dengan munculnya tampilan yang berbeda ketika system operasi tersebut dijalankan atau sebuah aplikasi digunakan. Selain memenuhi memori computer, akibat yang ditimbulkan juga sangat menggangu kinerja operasi computer.

Berbagai macam teknik dapat dilakukan guna mencegah dan menanggulangi terjangkitnya virus computer, salah satunya yaitu dengan cara

memasang program antivirus yang ada dipasaran dan banyak digunakan selama ini. Namun pada kenyataanya dalam proses pencegahan virus tersebut tidak dapat dibendung secara penuh, karena pemakaian antivirus yang sudah kadaluarsa (*out of date*). Sehingga virus masih tetap menyerang system computer. Sehingga apabila system computer yang digunakan sudah terlanjur terserang atau terjangkit virus, maka langkah yang perlu dilakukan adalah menanggulanginya. Dengan alasan tersebut maka dalam penelitian ini akan dibahas lebih detail tentang sIstem kerja dari virus computer melalui tahapan analisis penyerangan virus jenis worm W32/cyrax dan teknik penanggulangannya.

1.2. Tujuan Khusus

Tujuan khusus penelitian ini adalah :

a. Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:
    1. Melakukan penelusuran dan selajutnya menjelaskan faktor-faktor yang dapat menjadikan worm 32/cyrax dapat menyerang sistem komputer.
    2. Melakukan identifikasi dan menguraikan bagaimana cara kerja dan metode penyebaran dari virus komputer jenis worm tipe W32/Cyrax
    3. Melakukan identifikasi dampak yang diakibatkan dari serangan worm ini.
    4. Membuat sebuah prototipe perangkat lunak (software) yang dapat memberikan solusi penanggulangan terhadap bahaya yang ditimbulkan oleh worm W32/Cyrax.

5. Melakukan Pengujian efektifitas prototype antivirus yang dibangun dan dikembangkan terhadap perangkat PC, Jaringan, Ipad, dan Handphone.
6. Implementasi Hasil dan penyebarluasan software Antivirus (Sosialisasi)

1.3. Urgensi (Keutamaan) Penelitian

Urgensi dari penelitian ini adalah bahwa dampak penggunaan teknologi informasi yang begitu luas dan hampir dapat dinikmati semua lapis masyarakat, maka resiko yang ditimbulkan semakin luas. Untuk itu dalam penelitian ini diharapkan dapat memberikan keutamaan terhadap masyrakat pengguna komputer.

Manfaat yang diharapkan dan kontribusi dari Penelitian ini adalah :

1. Dapat mengetahui system kerja dan metode penyebaran virus secara umum, dan worm W32/Cyrax secara khusus, sehingga dapat menjaga dan mengantisipasi system computer agar terhindar atau mencegah dari serangan virus / worm.
2. Hasil penelitian dapat digunakan untuk menanggulangi, menghilangkan dan memberantas jenis virus worm 32/cyrax.
3. Hasil penelitian dapat digunakan sebagai salah satu atau alternatif referensi bagi pengguna atau pengembang antivirus/worm komputer apabila akan mengembangkan tipe anti virus/worm yang sejenis, misalnya untuk implementasi di perangkat handphone.

4. Mengurangi dan menghilangkan kekhawatiran para pengguna komputer terhadap ancaman serangan virus worm tersebut.
5. Sebagai pengembangan atau pengkayaan pengajaran pada matakuliah Sistem Keamanan komputer dan teknologi internet.
6. Hasil Software apalikasi anti virus worm ini nantinya dapat digunakan dan didapatkan secara gratis oleh semua kalangan seperti perusahaan, institusi, sekolah, dan sebaginya yang dapat diunduh melalui blog peneliti atau web institusi peneliti.

b. Luaran dari penelitian ini adalah:
    a. sebuah Perangkat Lunak (Software) Aplikasi Antivirus yang dapat mendeteksi adanya atau keberadaan Worm W32/Cyrax dan dapat menghapus atau menghilangkan worm tersebut.
    b. Pelaporan Penelitian
    c. Jurnal Ilmiah
c. Rencana diseminasi hasil penelitian :
    - Melalui seminar atau pertemuan ilmiah bidang teknologi informasi secara umum, dan keamanan komputer dan internet secara khusus.
    - Melalui jurnal publikasi ilmiah bidang teknologi informasi.
    - Melalui pengkayaan modul atau buku ajar kuliah keamanan komputer atau teknologi internet
    - Melalui Jejaring Sosial maya seperti Facebook dan twitter

BAB II
STUDI PUSTAKA

2.1. *State Of The art* (Tinjauan penelitian Terdahulu)

Inspirasi penelitian ini adalah berasal dari penelitian-peneltian sebelumnya, baik dari peneliti sendiri maupun dari penelitian orang lain. Seperti penelitian yang bahwa system keamanan computer dapat dilakukan dengan cara penyandian dokumen dengan model kriptografi. Namun perlu diperhatikan bahwa hasil nilai kriptografi yang berupa text-text yang sulit diterjemahkan belum tentu dari hasil penyandian, tapi juga dapat diakibatkan oleh virus computer yang seolah-olah melakukan penyandian, hal inilah yang perlu mendapat perhatian dan diwaspadai. (aji Supriyanto, 2009).

Penelitan lain menyatakan bahwa virus computer akan selalu berkembang karena begitu banyak pengguna yang menguasai teknik-teknik pemrograman. Melihat perkembangan teknik pemrograman virus yang begitu cepat dan semakin canggih, dipastikan muncul virus baru di masa depan yang menggunakan teknik tinggi. Akan selalu ada perbaikan dalam hal proses penyebaran diri, aksi maupun kecerdikan menghindari deteksi dari antivirus. Namun begitu pada dasarnya proses pendeteksian virus computer dapat dilakukan dengan cara pemanfaaan metode scan signature, metode heuristic, metode generic monitoring, metode integrity checkers, metode penjebak virus, dan metode emulator (http://victorx.4mg.com).

Beberapa teknik dapat digunakan untuk menghilangkan antivirus seperti menghapus dengan antivirus dikomputer lain, menghapus dengan system operasi lain,

dan mengahapus dengan system manual. Mengapus dengan system manual dapat dilakukan dengan cara mematikan proses yang dilakukan virus, selanjutnya melakukan pengembalian nilai default parameter sistem yang digunakan virus untuk mengaktifkan dirinya dan memblokir usaha menghapus dirinya, cegah virus aktif kembali dengan menghapus entry virus pada autorun dan startup Windows, melakukan installing antivirus kembali secara full scanning, dan melakukan restat system operasi kembali.(Wardana, 2006).

2.2. Penelitian Sebelumnya dan Buku yang Mendukung

Tabel 1. Penelitian pendukung yang dikerjakan sebelumnya dan akan diterapkan dalam penelitian multi tahun ini

Nama Peneliti / Tahun	Skim Penelitan	Judul Penelitian	Hasil penelitian	Rekomendasi
Aji Supriyanto, Heribertus, 2009	Unisbank	Rancang Bangun Keamanan Dokumen Kedinasan Elektronik Berbasis XML Menggunakan Kunci Publik	Pemakaian Kunci publik dalam pengiriman dokumen melalui jaringan/ internet dapat dilakukan dan akan menjadi lebih aman dibanding dengan pemakaian kunci privat, ini dikarenakan tidak	Pemakaian kunci public ini diharapkan untuk data yang menggunakan akses komunikasi lebih cepat, hal ini dikarenakan kapasitas enkripsi yang dilakukan akan

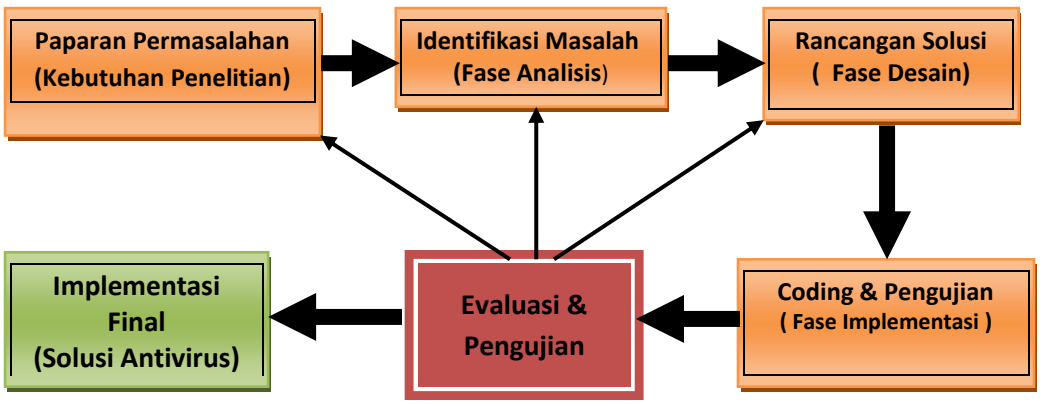
			tergantung terhadap kunci yang memang dipublikasikan	menghasilkan data yang lebih besar dibanding dengan kunci privat
Aji Supriyanto, Heribertus, 2007	Unisbank	Otentikasi Dokumen XML Model Multi Layer Menggunakan Algoritma RSA	Pemakaian Algoritma RSA dalam pengiriman dokumen melalui jaringan/ internet sangat aman dan sekaligus dapat digunakan sebagai dasar tandatangan digital	Agar pengiriman dokumen elektronik melalui media jaringan /internet menjadi aman perlu dilakukan enkripsi dengan kunci public dan selanjutnya ditandatangani secara digital.
Dwi Nugroho, Aji Supriyanto, 2008	Unisbank	Analisis Sistem Kerja Virus Jenis Worm Cyrax dan teknik pengendalianya dengan model heuristik	Identifikasi dan Model pengendalian Virus Jenis Virus Cyrax dapat dilakukan dengan sistem heuristic, sehingga dengan model penelusuran yang menyeluruh terhadap dokumen akan ditemukan	Agar sebuah data dapat aman dari ancaman jenis virus Cyrax ini, maka antivirus yang dihasilkan harus dapat dipasang dan mampu mendeteksi pada sebuah perangkat

			kode-kode khusus yang tidak sesuai dengan permulaan	yang membawa data dan terkena virus
Achmad Darmal	Jasakom	Computer Worm 1 & 2 Secret of Underground Coding	Kemampuan dasar virus komputer adalah mereproduksi dan distribusi, merekayasa sosial, menyembunyi-kan diri, mendapatkan informasi dan memanipulasi	Menggunakan jenis antivirus yang dapat mencegah, mengendalikan, dan menghilangkan sebuah data yang telah terkena virus tersebut
Tri Amperiy anto	Elex Media	Membuat dan Membasmi Worm-Virus	Tahapan siklus worm adalah peneyebaran, istirahat, aktif, dan eksekusi	Model pencegahan dan penaggulangan virus worm, harus dilakukan dengan cara mengenali pola siklus yang terjadi pada sebuah virus worm

BAB III
METODE PENELITIAN

3.1. Metode Penelitian yang Dikembangkan

Metode penelitian yang digunakan dalam penelitian ini adalah metode deskriptif analitik eksploratif, yaitu metode yang didasarkan pada studi kasus atau kejadian yang perlu dilakukan analisis permasalahan dan dilakukan perancangan untuk menemukan alternetif pemecahan masalahnya. Dikarenakan penelitian ini adalah termasuk penelitian rekayasa perangkat lunak, maka metode penyelesaian masalah digunakan metode pengembangan system terstruktur berbasis prototype. Fase-fase yang harus dilakukan dalam metode penelitian ini meliputi :



Gambar 3.1. Pengembangan Berbasis Prototyping

3.1.1. Inisiasi dan Identifikasi Permasalahan

Penelitian ini bertujuan untuk melakukan identifikasi dan analisis virus jenis Worm Cyrax W32, dan selanjutnya melakukan analisis sistem yang baru, melakukan desain antivirus yang dapat diimplementasikan dalam mencegah dan menangulangi ancaman worm cyrax tersebut.

Pada fase ini ditentukan pendataan sebagai berikut :

a. Objek Penelitian

   Objek penelitian ini adalah perangkat Komputer yang terserang atau terinfeksi virus jenis Worm W32/Cyrax

b. Jenis dan Sumber Data

   1. Data Primer. Data primer adalah data yang diperoleh langsung dari sumbernya. Dalam hal ini data primer meliputi sample computer yang terkena virus jenis worm W32/Cyrax.
   2. Data Sekunder. Data sekunder adalah data yang diperoleh secara tidak langsung, dalam hal ini data lebih dulu dikumpulkan dan dilaporkan oleh orang lain diluar penyelidikan sendiri, walaupun yang dikumpulkan itu merupakan data asli. Data sekunder antara lain dari journal, artikel-artikel, buku-buku, majalah, surat kabar, dan internet yang memuat dan membahas tentang worm W32.

c. Metode Pengumpulan Data

   1. Observasi. Yaitu melakukan pengamatan langsung terhadap objek komputer yang terkena serangan worm W32/cyrax. Dari pengamatan

langsung tersebut, kemudian dilakukan identifikasi apakah komputer tersebut terkena, serangan virus berjenis worm W32/cyrax atau terkena virus jenis yang lain. Yang selanjutnya dapat ditarik kesimpulan sementara dari keseluruhan objek yang diobservasi.

2. Studi Pustaka. Studi pustaka dilakukan dengan cara mengumpulkan dan melakukan pemahaman terhadap literatur-literatur yang melakukan bahasan tentang virus secara umum, dan worm W32 secara khusus. Pustaka yang digunakan berupa Journal, buku-buku, majalah, artikel, dan Internet.

d. Menentukan Variabel, instrumen, dan cara pengukuran

1. Menentukan variabel. Variabel yang digunakan dalam penelitian ini adalah varibel bebas (*independent variabel*) dan varibel terikat. Varibel bebas berupa pengamatan kepada sembarang komputer yang diduga terdapat virus/wormnya. Sedangkan variabel terikatnya adalah bahwa komputer yang diduga terserang tersebut harus menggunakan sistem operasi yang berbasis windows dan jenis virusnya dalah Worm W32/Cytrax.

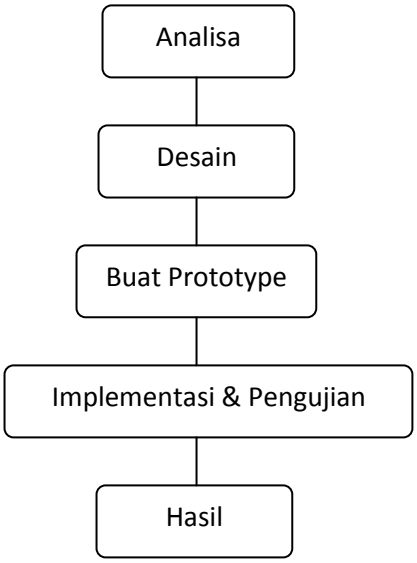
2. Instrumen yang digunakan. Instrumen penelitian baik untuk tahap analisis, desain, dan implementasi berupa personal komputer (PC) atau laptop dengan RAM minimal 256 MB dan Processor minimal P III. Sedangkan instrumen perangkat lunak untuk menganalisis adalah sistem operasi windows 2000 atau yang lebih baru, yang memiliki

perangkat registry yang lebih lengkap. Flask Disk yang berisi data sembarang yang diberi atau ditularkan Worm/Cytrax.

3. Teknik Pengukuran. Teknik Pengukuran untuk hasil analisis adalah dengan mendeteksi dan mengidentifikasi berubahnya nilai regisistry default. Sedangkan teknik pengukuran keberhasilannya adalah dengan hilangnya worm ketika dilakukan instalasi atau scanning antivirusnya.

3.1.2. Metode Pengembangan Sistem

Dalam pengembangan perangkat lunak (Software), peneliti memakai metode Prototype yaitu suatu proses pembuatan model dari perangkat lunak yang akan dibuat atau dikerjakan sehingga pemakai dapat mengetahui hasil yang didapat. Sedangkan tujuannya adalah mendefinisikan perangkat lunak yang akan dihasilkan tanpa menyertakan rincian pemasukan data, ataupun proses keluaran yang akan diperlukan (Roger S. Pressman, 2002:39-42). Proses yang terjadi dalam prototype dapat digambarkan sebagai berikut :



Gambar 3.2. Tahapan Metode Pengembangan Sistem

3.2. Analisis Sistem

Analisis merupakan proses menganalisa keperluan yang terdapat pada permasalahan yang ada. Melakukan analisis sistem yang lama yaitu menganalisa terhadap cara atau teknik penyerangan dan teknik pembuatan program worm W32/Cyrax. Sedangkan analisis untuk sistem yang baru dilakukan terhadap model-model yang dapat dilakukan untuk melakukan proses penghilangan atau penghapusan (*removal*) worm W32/Cyrax.

3.2.1. Analisis Sistem Dasar

Analisis sistem lama bertujuan untuk mengetahui dan mengidentifikasi jenis virus worm secara umum, mekanisme kerja, siklus kerja, dan teknik dasar kerja worm.

a.1. Definisi Worm

Sesuai dengan definisinya Virus worm, tidak sama persis dengan virus itu sendiri. Jika virus didefiniskan program yang memiliki kemampuan untuk berreproduksi, menulari program lain dan menjadikan file-file program tertular sebagai infector yang dapat merusak system computer. Dinamakan virus karena cara kerjanya mirip dengan virus biologis yang menginfeksi tubuh mahluk hidup. Sedangkan Worm merujuk pada program independent yang memiliki kemampuan untuk berreproduksi, menulari system computer dan walaupun mampu untuk menulari program lain namun tidak bertujuan untuk menjadikan file tertular tersebut sebagai suatu file infector.

Dari definisi diatas terlihat bahwa worm adalah suatu algoritma atau program yang mereproduksi diri sendiri dari system ke system dengan menggunakan media penyimpanan atau suatu jaringan. Worm tidak menginfeksi file program lain dengan tujuan menjadikan file terinfeksi tersebut sebagai file infector. Worm mampu bekerja tanpa interaksi user, bisa merusak sebuah data secara langsung atau menurunkan kinerja suatu system dengan *'mengikat'* sumberdaya system computer dan bahkan bisa mematikan sebuah jaringan. Berbeda dengan virus yang melakukan infeksi dengan *'menumpang'* pada file program lain, menunggu interaksi user dan menjadikan file terinfeksi sebagai file infector.

a.2. Sistem Kerja Worm

Mekanisme kerja dari Worm adalah sebagai berikut:

1. Kemampuan Reproduksi Dan Distribusi. Yaitu suatu kemampuan yang mutlak dimiliki suatu worm yntuk membuat salinan dirinya, sekaligus mendistribusikan salinan tersebut pada sistem yang lain baik melalui media penyimpanan seperti disket, USB flashdisk maupun melalui suatu jaringan komputer. Walaupun memiliki rutin untuk menginfeksi program lain namun tidak bertujuan menjadikan file program terinfeksi menjadi suatu file infektor. Pada awalnya worm dibuat dengan aksi memenuhi hardisk dan jaringan, namun seiring dengan perkembangan teknologi informasi hal ini akhirnya banyak ditinggalkan oleh para worm writer karena malah akan mengurangi kemampuannya untuk menyembunyikan diri, yang akan berakibat worm tersebut cepat ’terendus’ oleh advanced user atau bahkan perusahaan-perusahaan antivirus.
2. Kemampuan Rekayasa Sosial. Yaitu file infektor worm akan aktif saat user mengeksekusinya maka social engineeringatau rekayasa sosial menjadi hal yang sangat penting bagi suatu worm. Layaknya seorang penjual yang mati-matian merayu calon pembelinya maka wormakan ’merias’ programnya dengan icon dan nama yang sangat memikat agar user mengeksekusinya. Suatu worm bisa saja membuat salinan dirinya dengan nama file ’porno’ dan dengan gambar icon yang sangat tidak mencurigakan. Sebagai contoh worm lokal yang beredar di Indonesia

ada yang menggunakan icon folder, msword, excel, zip, notepad dll untuk mengelabuhi para korbannya.

3. Kemampuan Menyembunyikan Diri. Yaitu menjaga agar teteap tidak diketahui adalah penting untuk worm pada era sekarang ini agar tetap bertahan pada suatu sistem yang telah berhasil diinfeksi oleh suatu worm. Hal ini biasanya dilakukan dengan cara tidak menampilkan sesuatu dari worm baik berupa suara maupun tampilan visual, menyembunyikan program worm dari taskbar bahkan dari jendela tasklisk program seperti Task Manager.
4. Kemampuan Mendapatkan Informasi. Suatu worm harus bisa mendapatkan informasi yang ia butuhkan seperti jenis sistem operasi yang digunakan, direktori root, direktori System Windows bahkan worm mumnya memeriksa suatu sistem apakah terpasang antivirus atau tidak dan lebih jauh lagi worm akan berusaha mengenali jenis antivirus yang terpasang, memeriksa apakah sistem telah terinfeksi atau belum, dan sebagainya.
5. Kemampuan Mengadakan Manipulasi. Yaitu Umumnya manipulasi dilakukan oleh worm untuk bertahan hidup. Worm cenderung mengadakan manipulasi pada registry agar worm bisa tetap aktif saat komputer dihidupkan, bahkan manipulasi registry milik suatu antivirus agar tidak mengganggu worm tersebut. Tapi worm bisa saja

mengadakan manipulasi yang terlepas dari tujuan tadi, seperti mengubah volume label pada hardisk atau disket.

a.3. Siklus Worm

Siklus worm terdapat 4 fase, yaitu :

1. *Propagation Phase* (Fase Penyebaran). Pada fase ini worm akan membuat salinan dirinya ke suatu tempat, baik pada sebuah media penyimpanan seperti disket atau USB flashdisk, fix disk (tetap) atau jenis removable disk lainnya. Adapun penyebarannya dapat dilakkukan pada system local, jaringan atau internet.

2. *Dormant Phase* (Fase Istirahat/Tidur). Pada fase ini worm tidaklah aktif. Worm akan diaktifkan oleh suatu kondisi tertentu, semisal : tanggal yang ditentukan, kehadiran program lain/ dieksekusinya program lain, dan sebagainya. Tidak semua worm melalui fase ini.

3. *Trirerring Phase* (Fase Aktif). Difase ini worm tersebut akan aktif dan menetap pada memory, hal ini dipicu oleh metode *launcher* yang digunakan oleh worm tersebut dan setiap worm memiliki metode *launcher* yang berbeda-beda tergantung dari worm writernya masing-masing.

4. *Execution Phase* (Fase Eksekusi). Pada fase inilah worm yang telah aktif tadi akan melakukan fungsinya seperti menghapus file,

menampilkan pesan-pesan pada jam/tanggal tertentu, mebebani trafik jaringan, dan sebagainya.

a.3. Teknik Dasar Worm

Teknik Dasar Worm adalah sebagai berikut :

1. Metode *Polimorphic*. Metode polymorphic adalah suatu metode yang membuat file program worm atau virus berubah setiap pengeksekusian. Berubah disini bisa berupa perubahan pada isi program maupun ukuran program tersebut.

   Metode polymorphic biasanya digunakan oleh worm atau virus untuk menghindari scanning dari antivirus yang umumnya menggunakan checksum dalam mengenali worm atau virus.

2. *Droping File.* Metode drop file adalah suatu metode yang digunakan untuk mengekstrak suatu file tertentu dari file utama. Banyak sekali cara yang dapat digunakan untuk metode drop file ini dan umumnya cara tersebut selalu diakhiri dengan menggunakan fasilitas debug pada windows.

3. *Watcher*. Metode watcher adalah suatu metode yang membentuk suatu rangkaian program yang saling mengawasi satu sama lainnya, tidak hanya mengawasi keberadaan program tetapi juga mengawasi hal lain seperti suatu konfigurasi, keberadaan atau ketidakadaan suatu hal atau mengawasi suatu kejadian tertentu. Metode ini sering digunakan oleh

worm sebagai *'benteng pertahanan'*. Sebagai contoh suatu worm terdiri dari dari file A dan B. kedua file ini saling mengawasi satu sama lain jika file A aktif maka ia akan melakukan pengecekan apakah file B aktif, jika file B ternyata tidak aktif maka file A akan secara otomatis memanggil/mengaktifkan file B, begitu juga sebaliknya. Metode ini juga sering dikenal dengan nama *"File Ganda"*.

4. *Shell Spawning*. Metode ini merupakan salah satu trik dimana worm akan melakukan manipulasi nilai pada registry sehingga worm akan aktif jika user mengeksekusi suatu file dengan ekstensi tertentu seperti *.exe, *.txt, *.bat dan sebagainya. Berikut ini adalah beberapa lokasi key pada registry yang bisa digunakan untuk metode shell spawning :

Tabel 3.1. Registry Shell Spawning

Ekstensi	Lokasi Key
EXE	HKEY_CLASSES_ROOT\exefile\shell\open\command
BAT	HKEY_CLASSES_ROOT\batfile\shell\open\command
TXT	HKEY_CLASSES_ROOT\txtfile\shell\open\command
PIF	HKEY_CLASSES_ROOT\piffile\shell\open\command
COM	HKEY_CLASSES_ROOT\comfile\shell\open\command
REG	HKEY_CLASSES_ROOT\regfile\shell\open\command
SCR	HKEY_CLASSES_ROOT\scrfile\shell\open\command

5. Kompresi. Teknik ini digunakan oleh para worm writer dengan berbagai tujuan, diantaranya adalah agar ukuran file executable bisa dikecilkan sehingga mudah untuk didistribusikan dan juga sekaligus mengenkripsi file tersebut sehingga susah untuk di “unpack” oleh para ahli analisa worm atau virus.Teknik kompresi ini dilakukan dengan menggunakan tool pembantu yang sering disebut dengan istilah Executable Packer, Compactor atau Compressor. Contoh dari program ini seperti : UPX, ASPack, FSG, Petite dan sebagainya.

3.2.2. Analisis Sistem yang Dikembangkan

a.1. Analisis Kebutuhan Pengolahan

- Analisis Kebutuhan Data Masukan. Untuk kebutuhan masukan data ke dalam sistem yang akan dibuat berupa informasi mengenai drive atau partisi atau lokasi yang akan dilakukan *scanning* oleh program cyrax remover, data signature worm.
- Analisis Kebutuhan Proses. Untuk kebutuhan proses dalam sistem yang akan dibangun dapat dijabarkan menjadi beberapa proses :
    1. Memasukkan data dari informasi lokasi yang akan dilakukan pemeriksaan atau scanning worm akan otomatis tersedia pada saat program dijalankan
    2. Sistem akan melakukan proses scanning berdasarkan informasi lokasi /path yang akan di scan

3. Sistem akan mencatat data worm yang telah terdeteksi
4. Sistem akan melakukan proses penghapusan worm dan file-file yang dihasilkan worm beserta registry entry yang dibuat oleh worm

- Analisis Data Keluaran. Sistem yang dibangun nanti dapat memberikan informasi hasil scanning yaitu worm yang ditemukan dan telah di hapus.

a.2. Analisis Kebutuhan Hardware dan Software.

Kebutuhan hardware dan software yang akan digunakan untuk membangun program Cyrax Remover tersebut adalah:

- Kebutuhan Perangkat Keras (*hardtware*) : Seperangkat komputer setingkat Pentium 4 dengan RAM minimal 512MB, Harddisk 10GB, Modem, access Point,Handphone/ Ipad, Disk External, dan perangkat jaringan.
- Kebutuhan Perangkat Lunak (*Software*): sistem operasi Windows XP dan telah terinstall Microsoft Visual Basic 6.0, API Viewer, API Guide, Microsoft Office, dan dreamweaver, dan PCtools.

3.2.3. Analisis Sistem Worm Cyrax

Worm Cyrax pada dasarnya worm ini tidak banyak melakukan aksi-aksi seperti kebanyakan worm pada umumnya. Worm Cyrax ini hanya membuat duplikasi dirinya dengan random icon dan nama file (*filename*) pada suatu folder dalam jumlah yang cukup banyak. Worm ini tidak mengunci aplikasi seperti regedit, memanipulsi

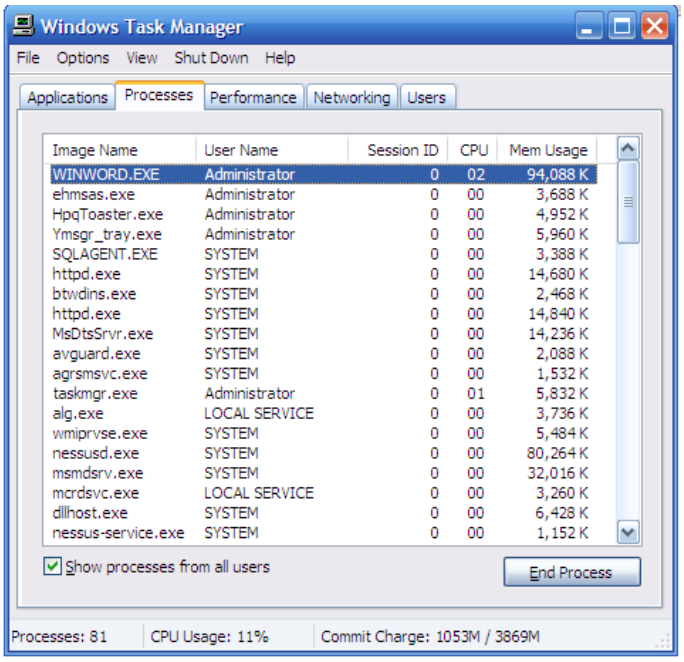
tab applications dan Process pada task manager. Spesifikasi virus Cyrax adalah sebagai berikut :

- Name : Cyrax
- Packer : AsPack 2.12
- FileSize : 78 Kbyte (packed), 168 Kbyte (unpacked)
- Compiler : MS Visual Basic 6.0
- Type : Worm

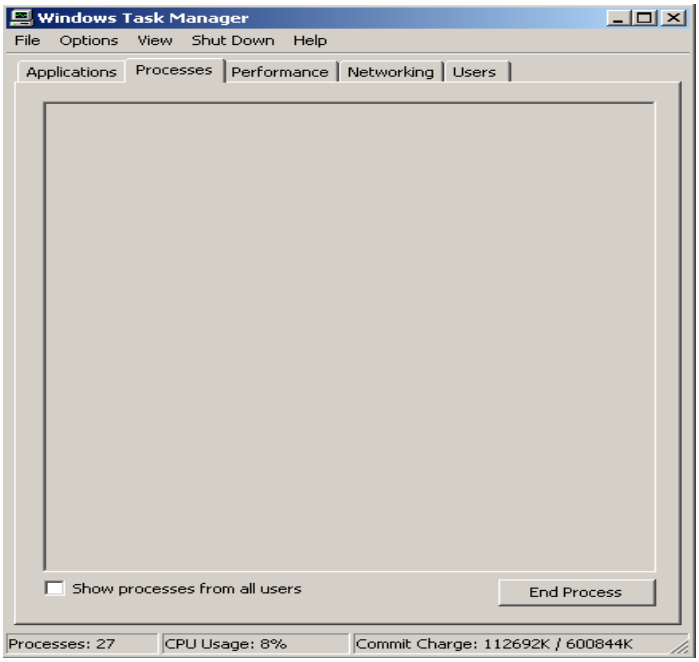
a.1. Ciri-ciri Worm Cyrax

Worm Cyrax memiliki cirri-ciri sebagai berikut :

1. Menggunakan random icon dan random filename pada file droppernya
2. Membuat duplikasi dengan memanfaatkan windows explorer
3. Menyembunyikan isi dari tab process dan application pada Task Manager dengan tujuan untuk mengelabuhi user atau korbannya sehingga proses dari worm tersebut tidak terlihat oleh user.

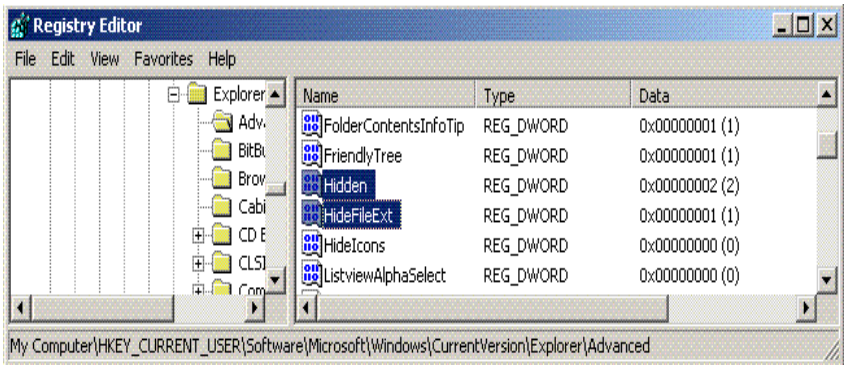


Gambar 3.3. Tampilan Normal Windows Task Manager (Sebelum Terkena Worm)



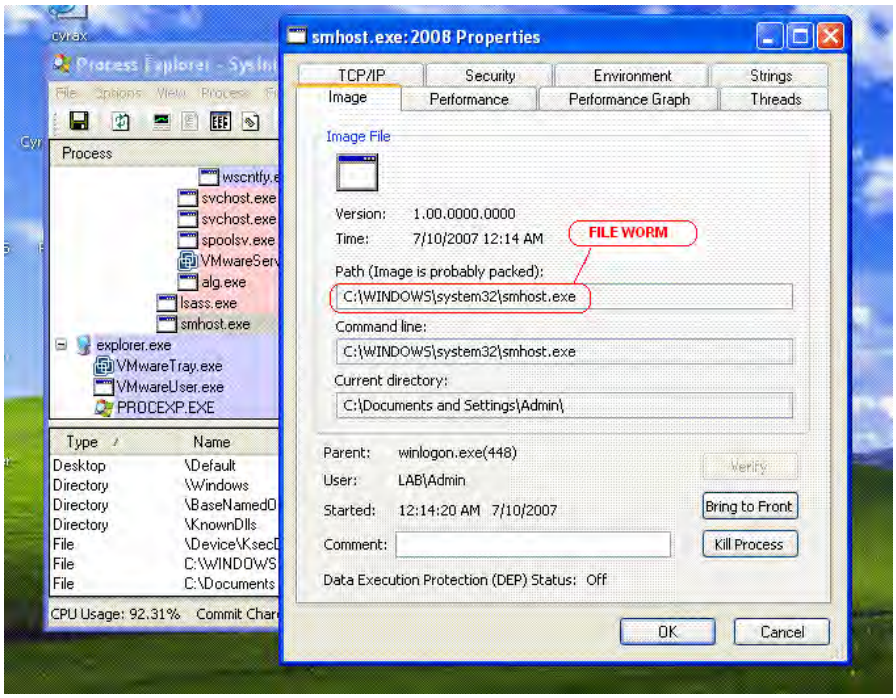
Gambar 3.4. Tampilan Windows Task Manager Setelah Terkena Worm

4. Melakukan beberapa manipulasi registry untuk mendukung aksinya seperti menyembunyikan ekstensi file, dan tetap aktif saat windows start up.



Gambar 3.5. Manipulasi registry

5. Membuat file induk dengan nama "smhost.exe, servlogon.exe"



Gambar 3.6. File induk worm dilihat dengan Process Explorer

6. Terjadinya Modifikasi Registry

- "HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit" dengan nilai"C:\WINDOWS\System32\userinit.exe;C:\WINDOWS\ System32\smhost.exe"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SRVstate" dengannilai "C:\WINDOWS\System32\smhost.exe"
- "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\RPCall" dengan nilai "C:\WINDOWS\System32\smhost.exe" dan "C:\Documents and Settings\(NamaUser)\Local Settings\Application Data\Microsoft\ servlogon.exe"
- "HKCU\Software\Microsoft\CommandProcessor\EnableExstentions' dengan nilai 0
- "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden" dengan nilai 0
- "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden" dengan nilai 2
- "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt" dengan nilai 1
- "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState\FullPath" dengan nilai 1
- "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState\FullPathAddress" dengan nilai 1
- "HKLM\Software\Microsoft\Windows\CurrentVersion\SystemFileProtection\ShowPopups" dengan nilai 0

a.2. Melakukan Analisa Worm

a.2.1. Menggunakan Tools Cracking Worm

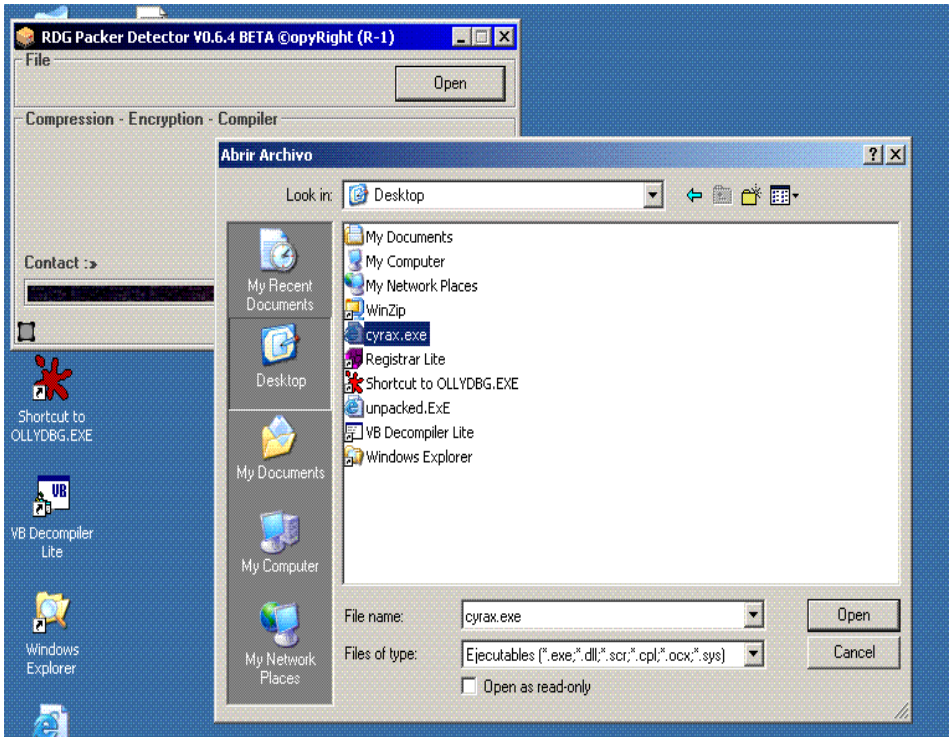
- RDG Packet Detector. Teknik ini untuk mengetahui worm tersebut memakai packer atau pembungkus atau pelindung worm. Biasanya

worm memakai packer untuk melindungi diri dari para cracker worm agar source codenya tidak terbongkar, RDG Packer Detector digunakan untuk keperluan tersebut.

- ASPack Die. Teknik ini untuk membongkar packer atau pelindung worm yang memakai perlindungan metode ASPACK
- Ollydbg. Teknik ini berguna untuk reverse engineering atau melihat source code worm. Walaupun hanya dapat dilihat dalam bahasa mesin atau assembly tapi ada keterangan - keterangan dari Ollydbg yang membantu untuk memahami isi worm tersebut
- VBDecompiler. Teknik ini berguna untuk mengetahui fungsi dan API apa yang digunakan oleh worm tersebut
- File Sample Worm

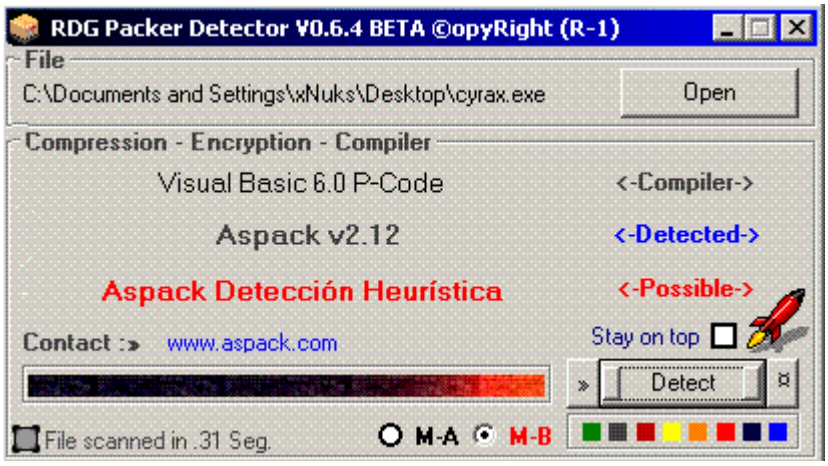
a.2.2. Melakukan Cracking Worm

Pada setiap langkah awal proses cracking worm atau virus maka harus dicari tahu apakah worm tersebut memakai packer atau tidak sehingga akan membantu proses cracking selanjutnya. Aktifkan RDG Packet Detector untuk mengetahui worm cyrax memakai compiler dan packer apa sehingga dapat dipiilih program unpacker untuk membongkarnya, seperti terlihat pada gambar berikut :



Gambar 3.7. Pemilihan file target

Kemudian bentuk tampilan dari RDG Packet Detector akan seperti gambar berikut:

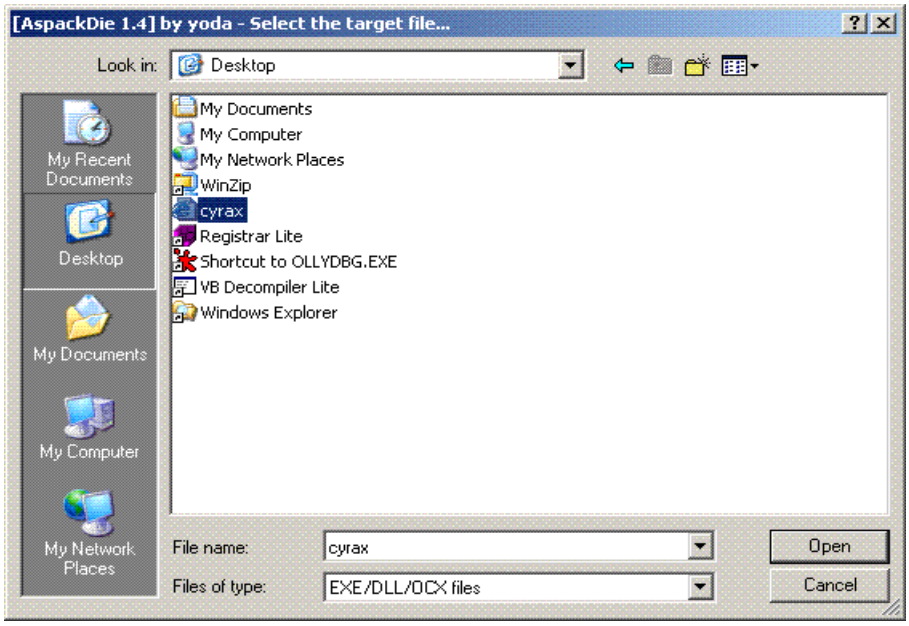


Gambar 3.8. Hasil deteksi RDG Packet Detector

Dari hasil diatas didapatkan beberapa keterangan yaitu :

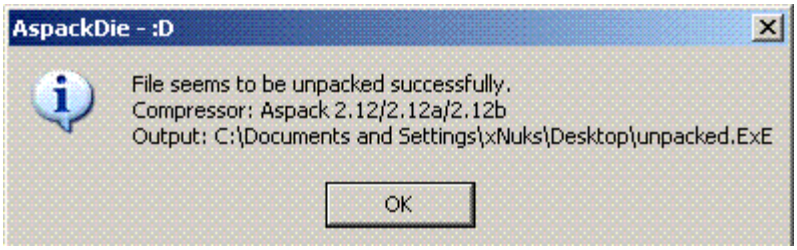
1. Visual Basic 6.0. Maksud dari keterangan diatas adalah kompiler yang dipakai worm, bisa jadi bahasa pemrograman atau untuk meng-compile code menjadi .exe. Karena di sini ditulis Visual Basic 6, maka kita dapat menggunakan vb Decompiler sebagai software reverse engineering-nya
2. ASPack 2.12. Maksud dari keterangan diatas adalah packer atau packing yang digunakan sebagai pelindung worm atau pembungkus kode worm agar kode-kodenya tidak dapat dilihat oleh pemburu worm. Karena di sini memakai Aspack v2.12 maka kita dapat memakai software aspackdie untuk membongkar pelindungnya
3. Aspack Detection Heuristic. Maksud dari keterangan diatas adalah Heuristic atau pengacakan dari data virus tersebut

Langkah selanjutnya mencoba menghancurkan pembungkus atau packer dari kode – kode tersebut, untuk menghancurkannya jalankan software aspackdie dan pilih file yang ingin dihancurkan packernya, kemudian pilih Open.



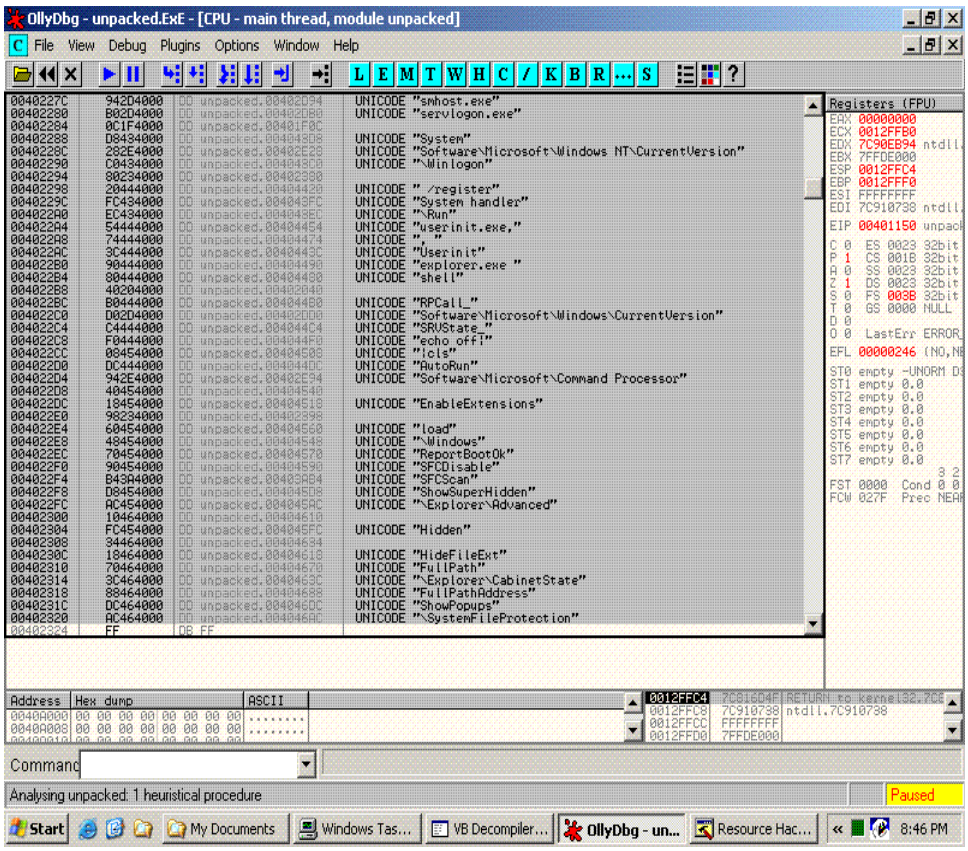
Gambar 3.9. Pemilihan file target dengan Aspackdie v1.4

Jika berhasil File akan disimpan oleh Aspackdie sebagai unPacked.exe dan akan muncul pesan seperti gambar berikut :



Gambar 3.10. Pesan dari Aspackdie

Langkah selanjutnya kita buka ollydbg untuk membedah isi worm tersebut, kemudian pilih file unpacker.exe tadi untuk dibuka isinya



Gambar 3.11. Worm dibuka dengan Ollydbg

Seperti gambar diatas sebenarnya isi dari file unpacked.exe sangat banyak jadi disini di ambil beberapa bagian.dari hasil analisa menggunakan ollydbg. Terdapat beberapa string yang digunakan oleh worm cyrax yaitu:

1. String yang digunakan untuk random filename:

"Daftaranggota,datakaryawan,laporanharian, pivot able"
"data pegawai,backup_database,data keuangan"
"cv,hackingtutorial,proposal,surat perjanjian, adendum"
"artis,hot image,ini aku lho,photo bosku,"
"winampsetup3,vbdecompiler,mssp4forxp,keygen xp"
"windowslogo,mybrother,artisofthemonth,photoseru"
"sepultura-root,nirvana-drainyou,samson-naluri-lelaki,radja-yakin,ungu-kenangan terindah"
"lagu sunda,lagu barat,daftar top10 indo,best barat"

"arsip bulan juni2006,my data,get data back,my artis pic"
"tutorialhacking,manualguidefinger,allaboutcracking,trojan maker"
"backupdata,winamp6.0 full,firefox1.6,source baru"
"iso2000,what the hell,hot animal,apa ya"
"commands,net86,winloggon,star,smartdrvs, telnet"
"MyDocument,MyPicture,Windows,Winnt,System32,System,Progra mFiles,Inetpub, Temp,Tmp,Download"
"Readme,Eula,logevent,manualguide,Bacadonk, Catatan"
"xls,mdb,doc,gif,cmd.exe,jpg,mp3,m3u,rar,pdf,zip,lnk,txt"
"cyrax."

2. String untuk proses penggandaan file pada windows explorer
"Buat Duplikasi di directory: "
"ExploreWClass"
"WorkerA"
"WorkerW"
"ReBarWindow32"
"ComboBoxEx32"
"ComboBox"
"Edit"
"IEFrame"
"Navigation Bar"
"Address Band Root"

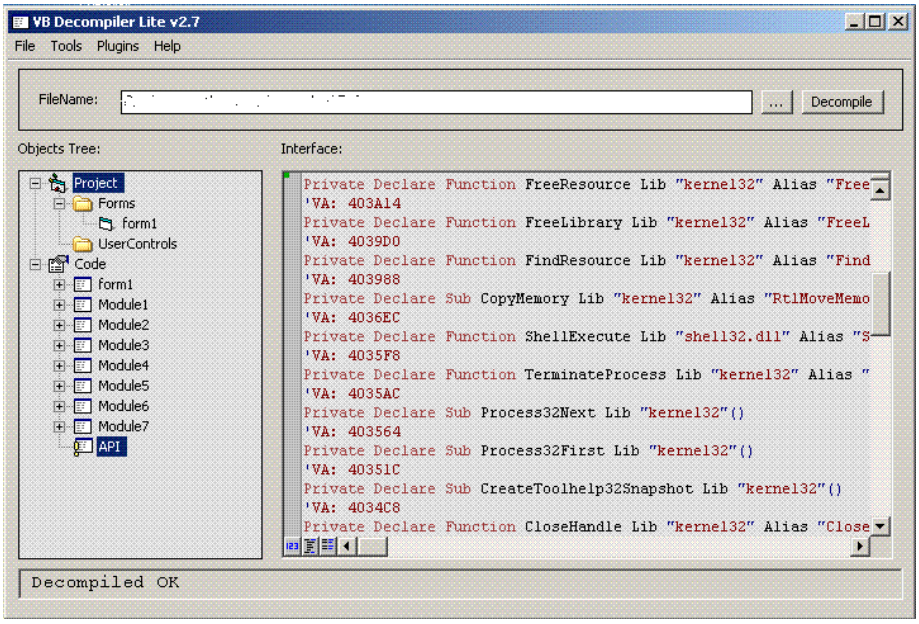
3. String manipulasi Task Manager
"Windows Task Manager"
"#32770"
"Processes"
"SysListView32"
"Tasks"

4. String file induk worm
"smhost.exe"
"servlogon.exe"

5. String Manipulasi Registry
"smhost.exe"
"servlogon.exe"
"\Application Data\Microsoft\"
"userinit.exe,"
","
"Userinit"
"Software\Microsoft\Windows NT\CurrentVersion"
"\Winlogon"
"Shell-"
"Software\Microsoft\Windows\CurrentVersion"
"\Run"
" /register"

"SRVState_"
"RPCall_"
"EnableExtensions"
"Software\Microsoft\Command Processor"
"ShowSuperHidden"
"\Explorer\Advanced"
"Hidden"
"HideFileExt"
"FullPath"
"\Explorer\CabinetState"
"ShowPopups"
"\SystemFileProtection"

Untuk mengetahui fungsi-fungsi API yang digunakan dapat menggunakan software VBDecompiler. Walaupun source codenya tidak terlihat "FullPathAddress"semua tetapi kita dapat mempelajari fungsi APInya. Pilih file yang ingin di decompiler, yaitu file yang telah dihancurkan packernya tadi yaitu unpacker.exe. kemudian klik Decompile, maka akan terlihat seperti gambar berikut :



Gambar 3.12. VBDecompiler

Dari gambar diatas worm cyrax memakai bermacam fungsi API untuk melakukan aksinya. Seperti kebanyakan worm yang dibuat dengan Visual Basic. Berikut beberapa fungsi API yang digunakan oleh worm Cyrax:

```
Private Declare Function WNetAddConnection2 Lib "mpr.dll"
Private Declare Function lstrcpy Lib "kernel32"
Private Declare Function lstrlen Lib "kernel32"
Private Declare Function WNetCloseEnum Lib "mpr.dll"
Private Declare Function WNetEnumResource Lib "mpr.dll"
Private Declare Function WNetOpenEnum Lib "mpr.dll
Private Declare Function LoadLibraryEx Lib "kernel32"
Private Declare Function LoadResource Lib "kernel32"
Private Declare Function LockResource Lib "kernel32"
Private Declare Function SizeofResource Lib "kernel32"
Private Declare Function FreeResource Lib "kernel32"
Private Declare Function FreeLibrary Lib "kernel32"
Private Declare Function FindResource Lib "kernel32"
Private Declare Sub CopyMemory Lib "kernel32"
Private Declare Function ShellExecute Lib "shell32.dll"
Private Declare Function TerminateProcess Lib "kernel32
Private Declare Sub Process32Next Lib "kernel32"()
Private Declare Sub Process32First Lib "kernel32"()
Private Declare Sub CreateToolhelp32Snapshot Lib "kernel32"()
Private Declare Function CloseHandle Lib "kernel32"
Private Declare Function GetParent Lib "user32"
Private Declare Sub OpenProcess Lib "Kernel32.dll"()
Private Declare Function DestroyWindow Lib "user32"
Private Declare Function PostMessage Lib "user32"
Private Declare Function RegEnumValue Lib "advapi32.dll"
Private Declare Function RegEnumKeyEx Lib "advapi32.dll"
Private Declare Function RegSetValueEx Lib "advapi32.dll"
Private Declare Function RegQueryValueEx Lib "advapi32.dll".
Private Declare Function RegOpenKey Lib "advapi32.dll"
Private Declare Function RegCreateKey Lib "advapi32.dll"
Private Declare Function RegCloseKey Lib "advapi32.dll"
Private Declare Function RegDeleteValue Lib "advapi32.dll"
Private Declare Function GetWindowsDirectory Lib "kernel32"
Private Declare Function GetSystemDirectory Lib "kernel32"
Private Declare Function GetComputerName Lib "kernel32"
```

```
Private Declare Function LockWindowUpdate Lib "user32"
Private Declare Function CopyFile Lib "kernel32"
Private Declare Sub PathIsDirectoryA Lib "shlwapi.dll"()
Private Declare Function SendMessage Lib "user32"
Private Declare Function FindWindowEx Lib "user32"
Private Declare Function FindWindow Lib "user32"
Private Declare Function WindowFromPoint Lib "user32"
Private Declare Function GetCursorPos Lib "user32"
Private Declare Function GetForegroundWindow Lib
Private Declare Function GetFileTitle Lib "comdlg32.dll
Private Declare Function GetVersionEx Lib "kernel32"
```

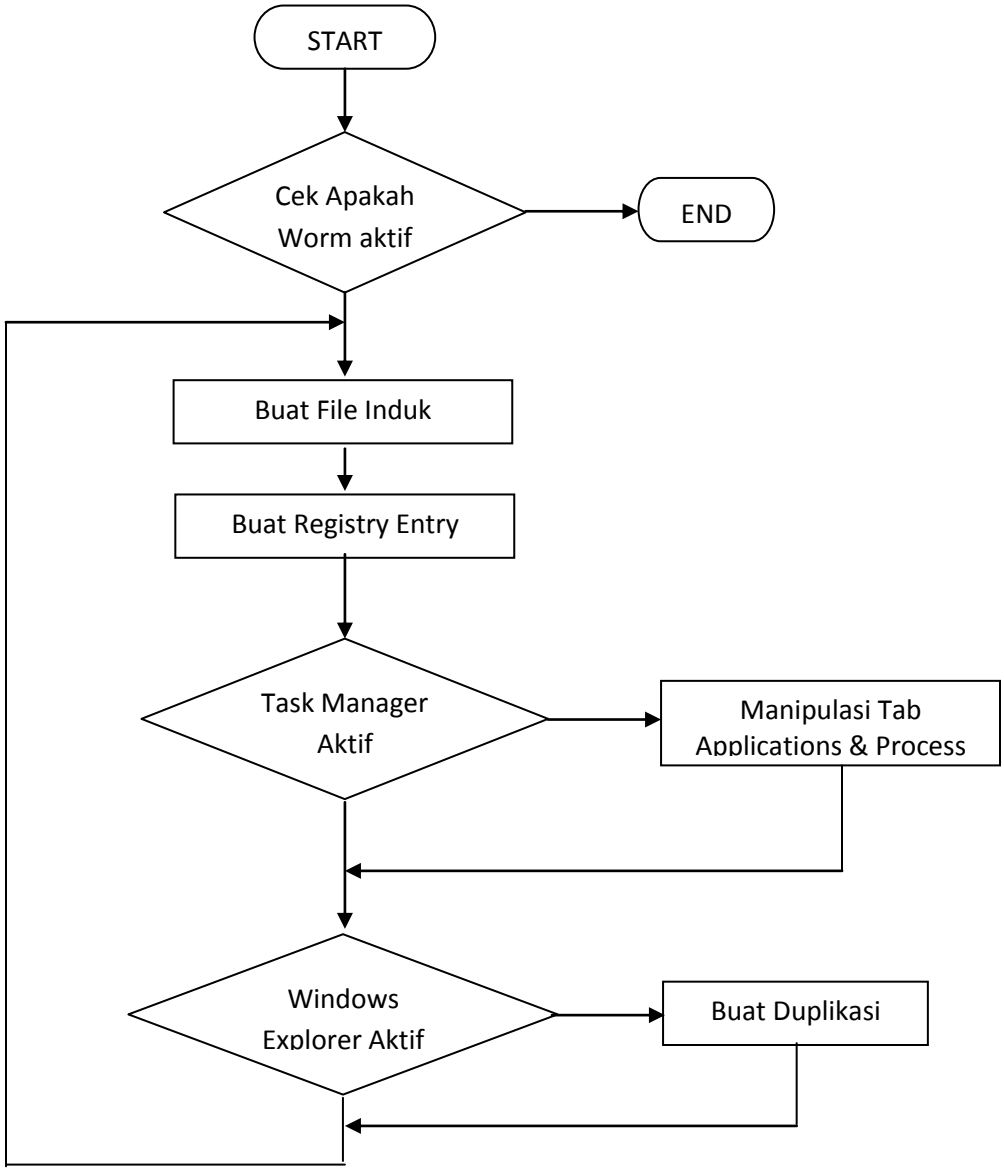
3.2.4. Hasil Analisis

Dari hasil analisa dengan pengamatan langsung terhadap objek dan dengan menggunakan beberapa tools diatas, maka didapatkan hasil yaitu cara kerja dari worm adalah sebagai berikut:

a. Melakukan pengecekan apakah ada program worm sudah aktif. Jika ternyata program worm telah aktif maka program tidak akan jalan/aktif sedangkan jika tidak ditemukan maka worm akan aktif dan melakukan berbagai aktifitasnya.
b. Worm akan membuat file induk dengan nama “Servlogon.exe” dan “smhost.exe”
c. Membuat registry entry agar worm tetap aktif dalam system korbannya.
d. Melakukan monitoring terhadap aplikasi Task Manager. apabila task manager aktif maka worm akan melakukan manipulasi pada tab Process dan Aplications milik task manager.

e. Melakukan monitoring windows explorer serta membuat file dropper pada folder yang dibuka dengan random filename dan random icon

Dari Tahapan analisis diatas, maka flowchart analisis worm Cyrax dapat digambarkan sebagai berikut.



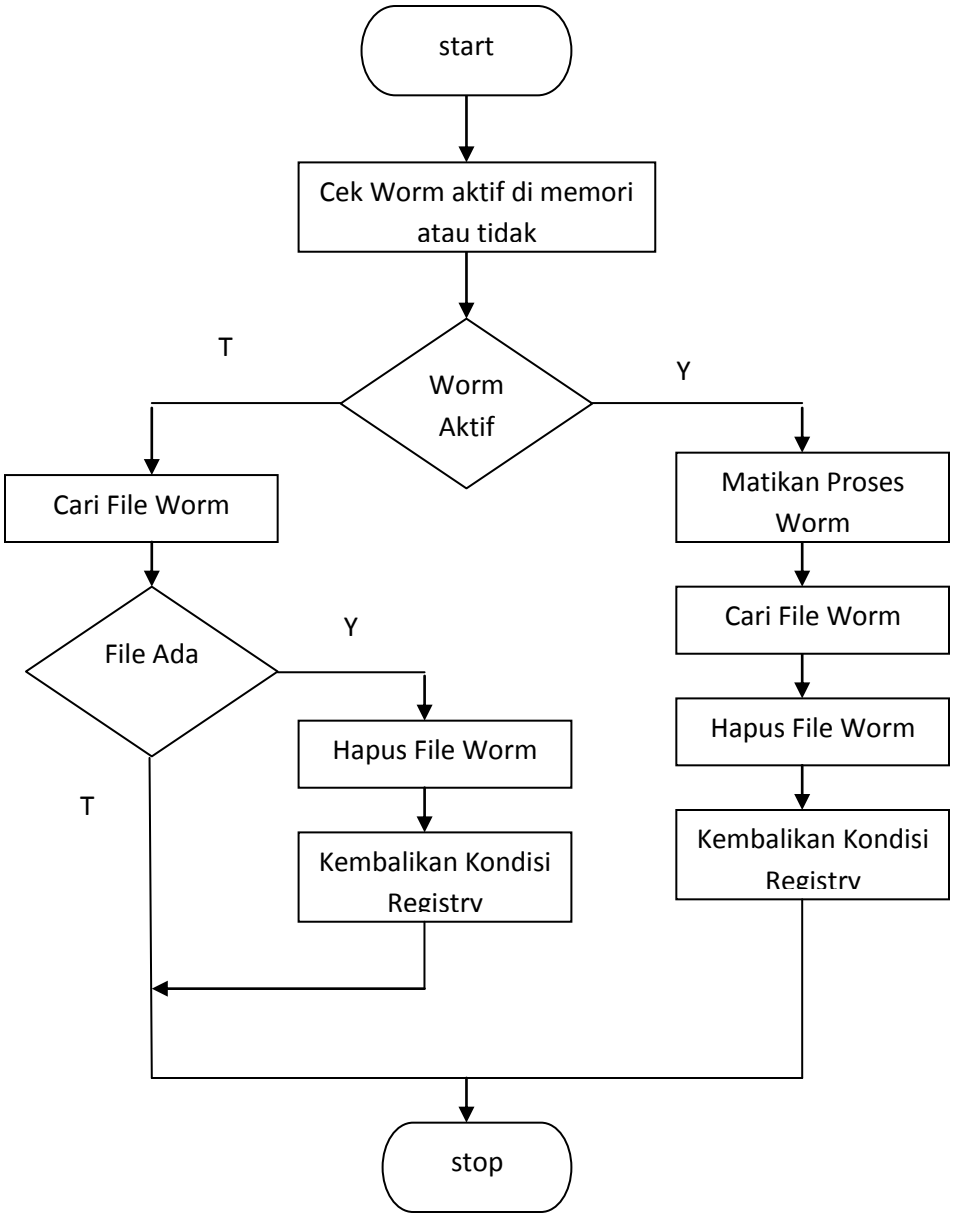
Gambar 3.13. Flowchart Pengecekan Worm Cyrax

3.3. Desain Sistem

Desain sistem merupakan kegiatan yang dilakukan dari hasil analisis sistem sebelumnya. Proses perancangan dari model atau prototype permasalahan yang ada, yaitu dengan membuat prototipe perangkat lunak (software) program removal untuk worm W32/Cyrax. Desain sistem ini meliputi desain proses dan desain antarmuka.

3.3.1. Desain Proses

Desain proses merupakan desain yang menggambarkan proses operasi sistem yang digambarkan dengan menggunakan Bagan Alir Program *(Program Folwchart).* Bagan Alir Program *(Program Flowchart)* merupakan bagan yang menjelaskan secara rinci langkah – langkah dari proses program. Bagan Alir Program *(Program Flowchart)* dibuat dari derifikasi bagan alir sistem. Perancangan proses ini merupakan perancangan operasi program Cyrax Removal yang akan digunakan untuk proses scanning worm dan menghapus file worm yang dapat dilihat pada gambar dibawah.



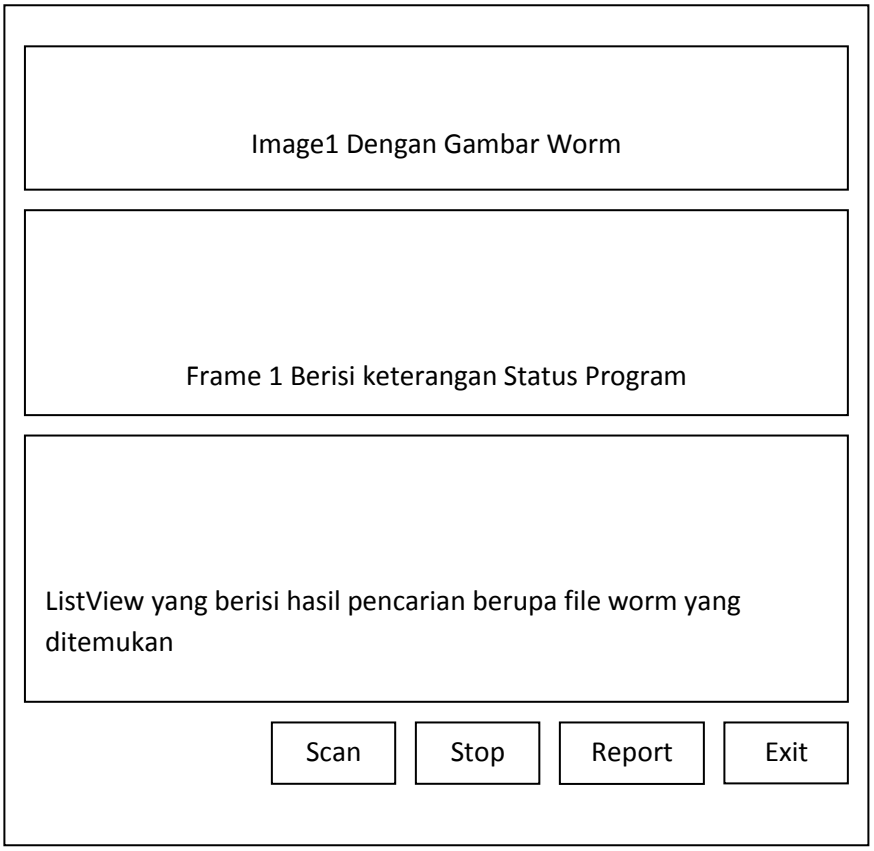
Gambar 3.14. Flowchar Program Worm W32/Cyrax Remover

3.3.2. Perancangan Antar Muka

Perancangan antar muka (*User Interface* /UI) merupakan model rancangan yang digunakan untuk memberikan gambaran visual tentang aplikasi yang digunakan

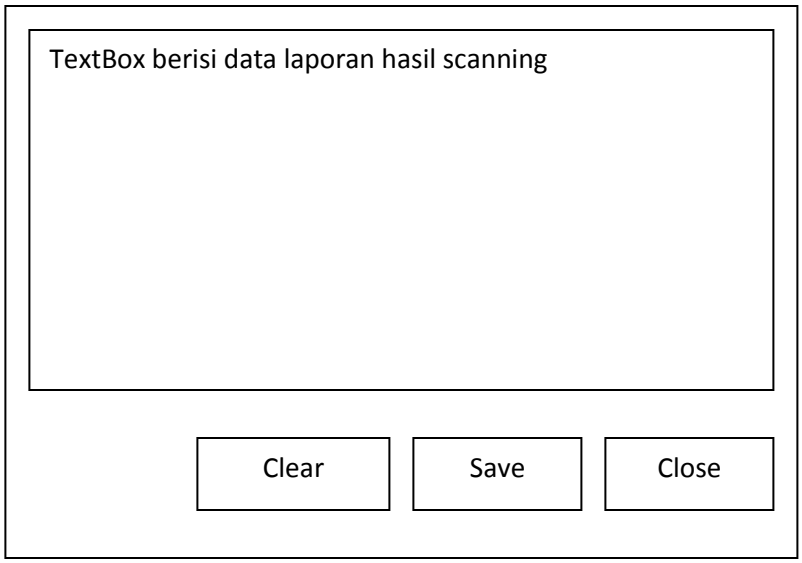
oleh user. Dalam rancangan UI ini, digunakan satu buah form utama berisi beberapa alternatif atau pilihan tombol – tombol button untuk melakukan proses scanning, menghentikan proses scanning dan menutup program. Rancangan tampilan antarmuka adalah sebagai berikut.

a. Tampilan Form Utama



Gambar. 3.15. Rancangan form utama

b. Tampilan Form Log

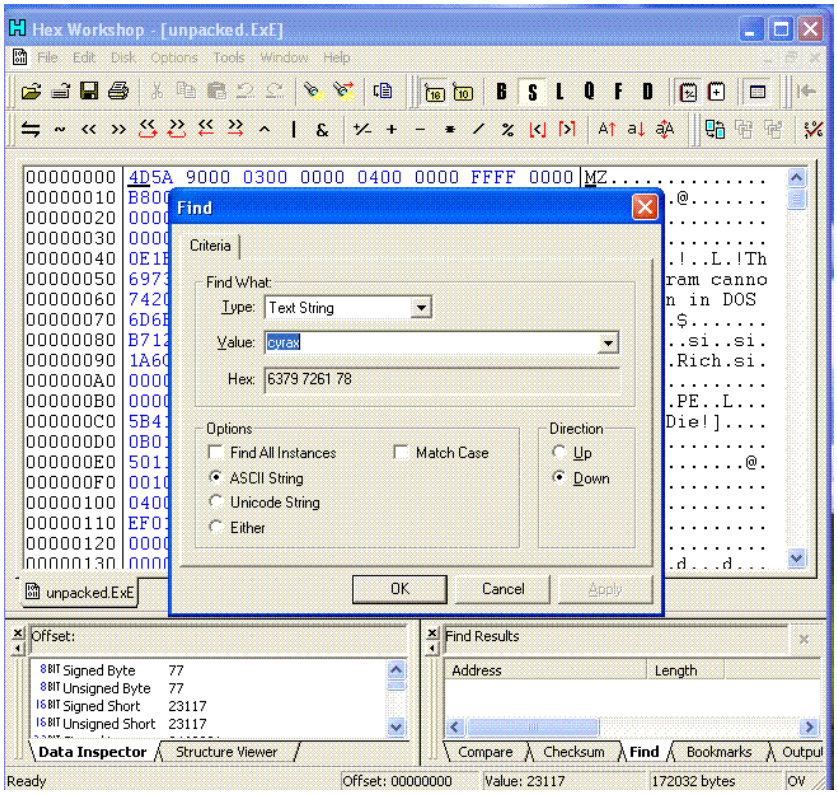


Gambar. 3.16. Rancangan form log

3.3.3. *String Signature*

String Signature merupakan teknik melindungi identifikasi beberapa string pada body file, sehingga sulit untuk mengetahui string apa yang digunakan oleh suatu antivirus, berapa string yang digunakan oleh antivirus tersebut, berapa panjang string tersebut, dan berapa jumlah section signature tersebut. Terdapat ratusan bahkan ribuan dan jutaan kemungkinan yang bisa terjadi. Untuk mendapatkan string signature dalam penelitian ini digunakan program Hex Workshop dengan cara melakukan unpacking file worm lalu membukanya menggunakan aplikasi Hex Workshop. Disini dapat mengambil data string "cyrax" yang terdapat pada posisi byte ke 1355 (heksa) atau 4949 (decimal) karena data tersebut menurut penulis cukup

akurat untuk dijadikan data signature mengingat terdapat string “cyrax” yang merupakan nama dari worm tersebut. Berikut adalah gambar dari proses pencarian data signature dari worm cyrax:



Gambar. 3.17. Pencarian String Signature

BAB IV

IMPLEMENTASI SISTEM

4.1. Kebutuhan Perangkat Implementasi

4.1.1. Kebutuhan Hardware dan Software

Sebelum sistem diimplmentasikan dan di uji coba, maka kebutuhan perangkat keras (*Hardware*) dan perangkat lunak (*software*) harus dipersiapkan terlebih dahulu. Selain itu juga termasuk perangkat jaringan untuk menguji antivirus yang pada sebuah perangkat jaringan. Spesifikasi hardware dan software pada perangkat komputer Personal (*personal computer/PC*) hampir serupa dengan Komputer yang digunakan pada jaringan lokal komputer.

Kebutuhan hardware dan software yang digunakan untuk melakukan ujicoba program Cyrax Remover tersebut antara lain :

a. Perangkat keras komputer dengan spesifikasi minimum :

- Intel Pentium 3 dengan Clock Speed 1200 Mhz
- Harddisk 40 GB
- Monitor komputer SVGA
- RAM 256 MB
- CD ROM atau Flash Disk

b. Perangkat Lunak dengan spesifikasi :

- Sistem Operasi Microsoft Windows XP
- Beberapa Software Spreeadsheet
- Sample Worm Cyrax

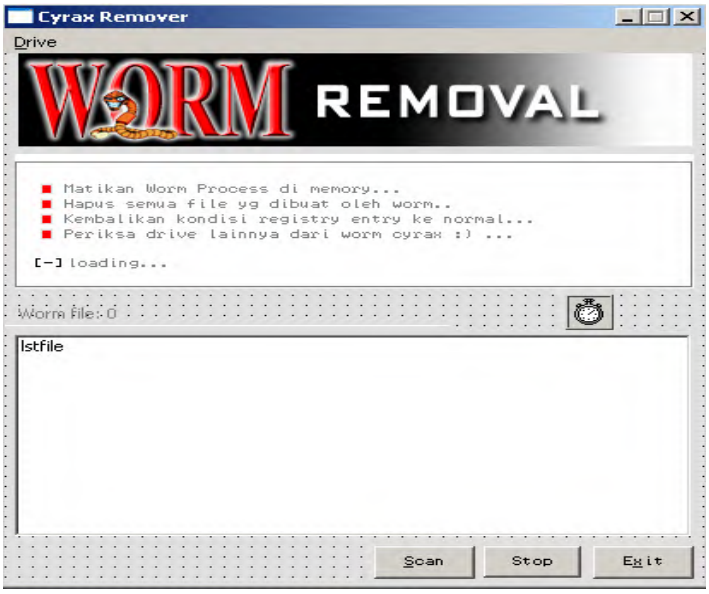
c. Perangkat Jaringan

- Spesifikasi hampir sama dengan a dan b diatas, dan ditambah dengan pheripheral jaringan komputer.

4.1.2. Kebutuhan Aplikasi Sistem

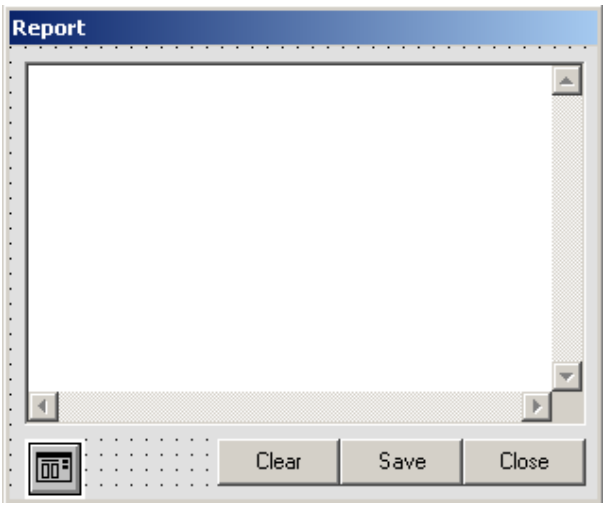
Aplikasi sistem merupakan perangkat lunak aplikasi yang akan digunakan untuk alat utama pengujian. Tampilan utama program aplikasi adalah seperti berikut.

a. Program Utama



Gambar 4.1. Tampilan Utama Aplikasi Cyrax Removal

b. Tampilan Scanning Report

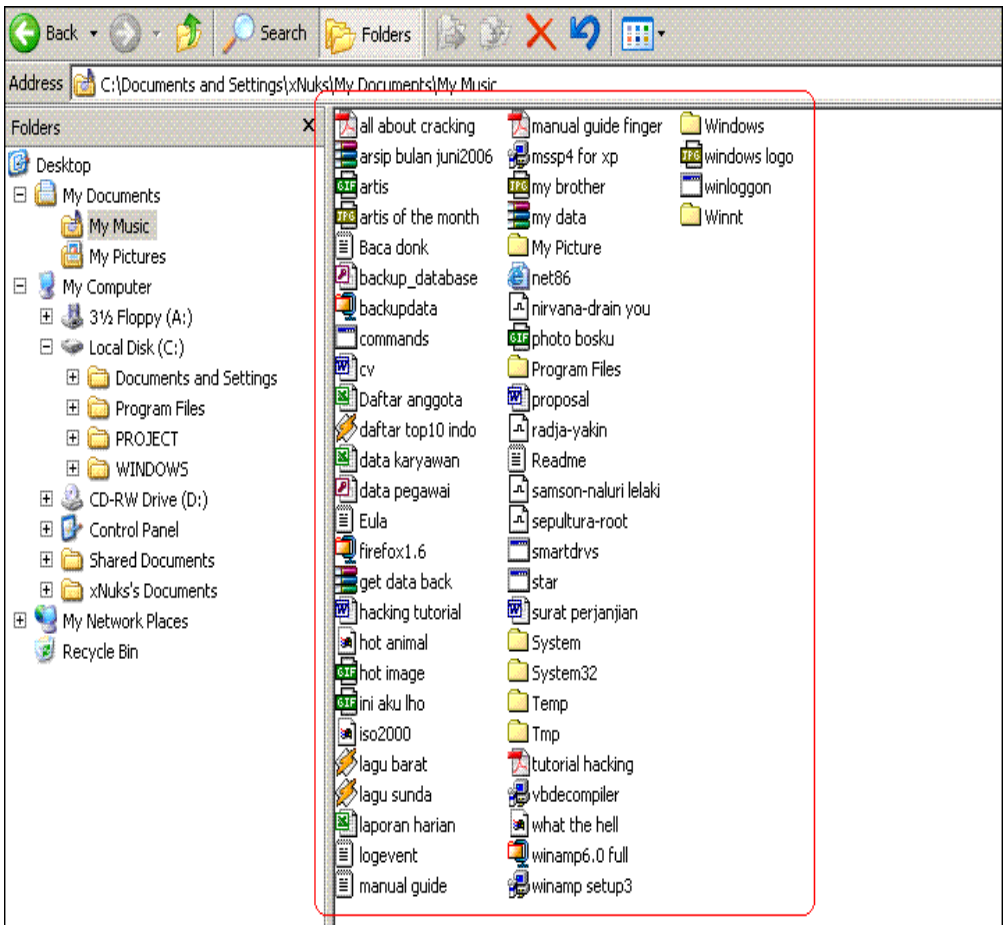


Gambar. 4.2. Tampilan form log

4.2. Pengujian dan Hasil

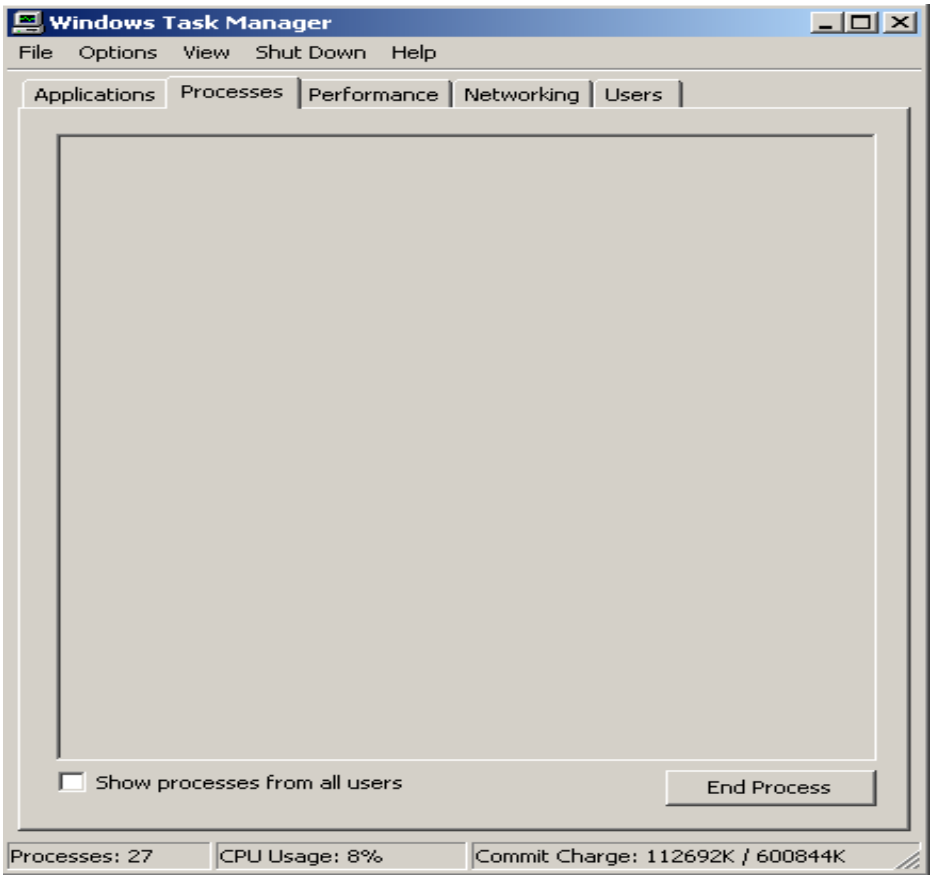
4.2.1. Uji Coba Program Removal

Tahap pengujian dilakukan setelah tahap analisis dan desain sistem selesai dilaksanakan. Pada tahab uji coba ini dilakukan pada sebuah komputer yang sebelumnya dengan sengaja telah diinfeksi dengan worm Cyrax. Sebagai gambaran, berikut ini merupakan tampilan gambar dari komputer yang telah terinfeksi worm cyrax beserta manipulasi – manipulasi yang terjadi akibat dampak dari aktifitas worm cyrax tersebut sewaktu belum dilakukan proses scanning menggunakan program Cyrax Remover.



Gambar. 4.3. Aktifitas worm Cyrax

Sedangkan Gambar berikut merupakan salah satu bentuk manipulasi worm cyrax terhadap aplikasi Task Manager.

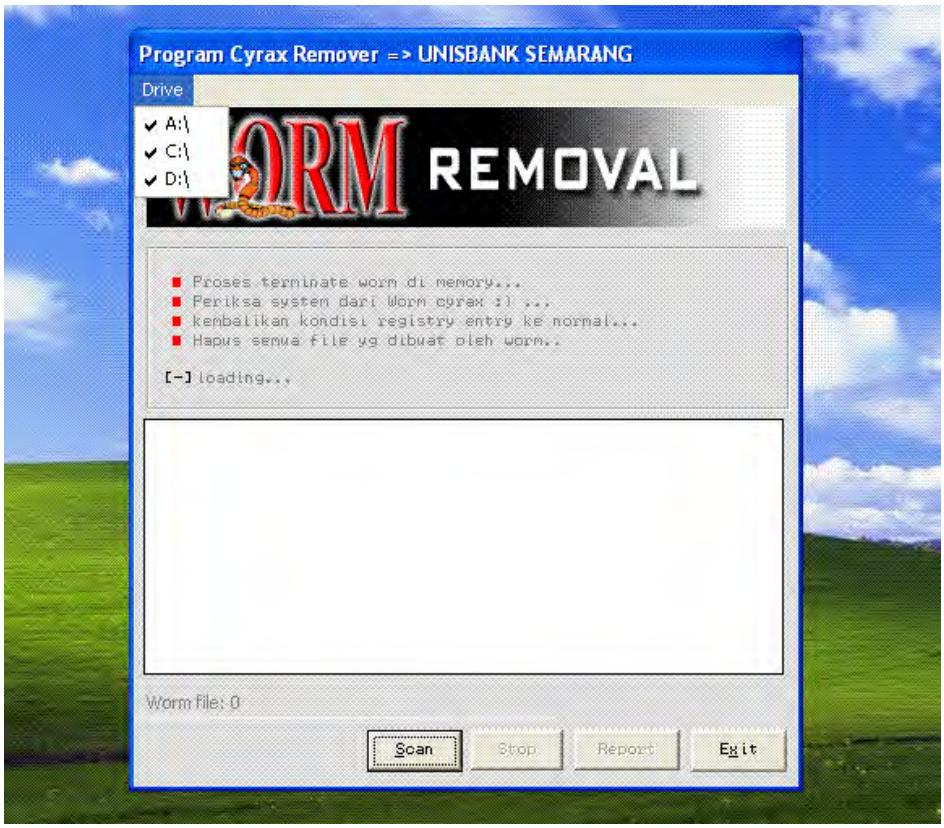


Gambar. 4.4. Manipulasi worm terhadap Task Manager

Dan selanjutnya Langkah-langkah berikut merupakan tahapan dari proses scanning menggunakan program Cyrax Remover untuk mengatasi dampak atau aktifitas dari worm Cyrax, yaitu:

a. Pemilihan lokasi scanning

   Program akan secara otomatis mendeteksi drive yang ada pada komputer. Penggantian drive yang akan di scan dapat dilakukan secara manual

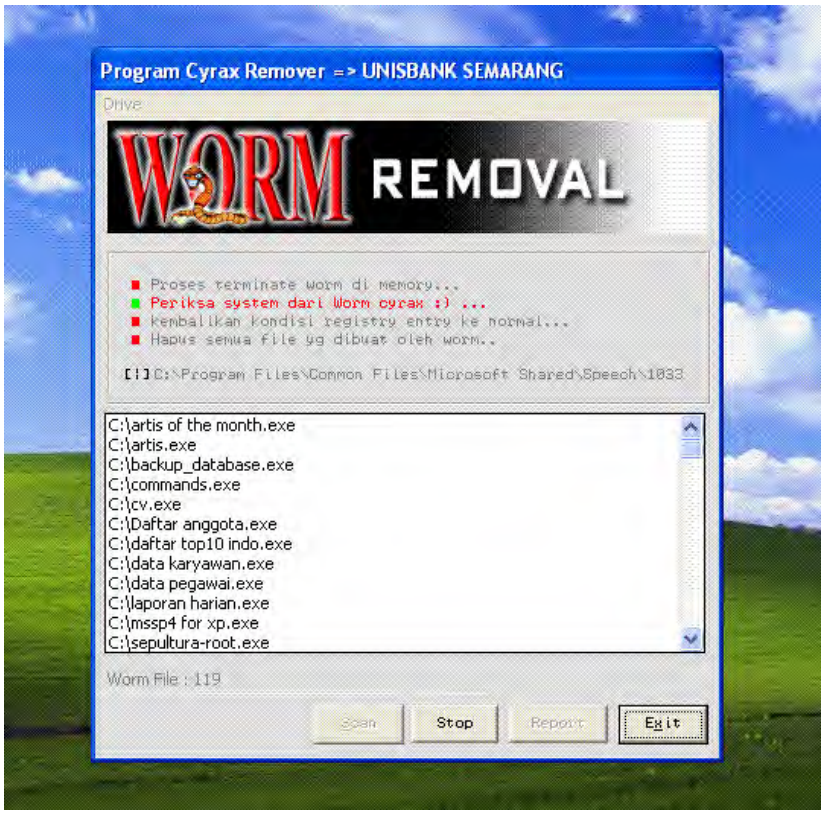


Gambar 4.5. Pemilihan lokasi scanning

b. Proses Scanning pada lokasi yang telah ditentukan

Setelah ditentukan lokasi scanning maka program akan melakukan scanning atau pencarian dari worm. Pertama –tama program akan melakukan pengecekan apakah worm aktif dalam memori computer. Jika ternyata ditemukan worm aktif maka program akan melakukan proses terminating terhadap proses dari worm Cyrax kemudian program akan melakukan pencarian file-file dropper dari worm, menghapusnya jika ditemukan serta program akan menghapus registry entry yang dibuat oleh worm dimana

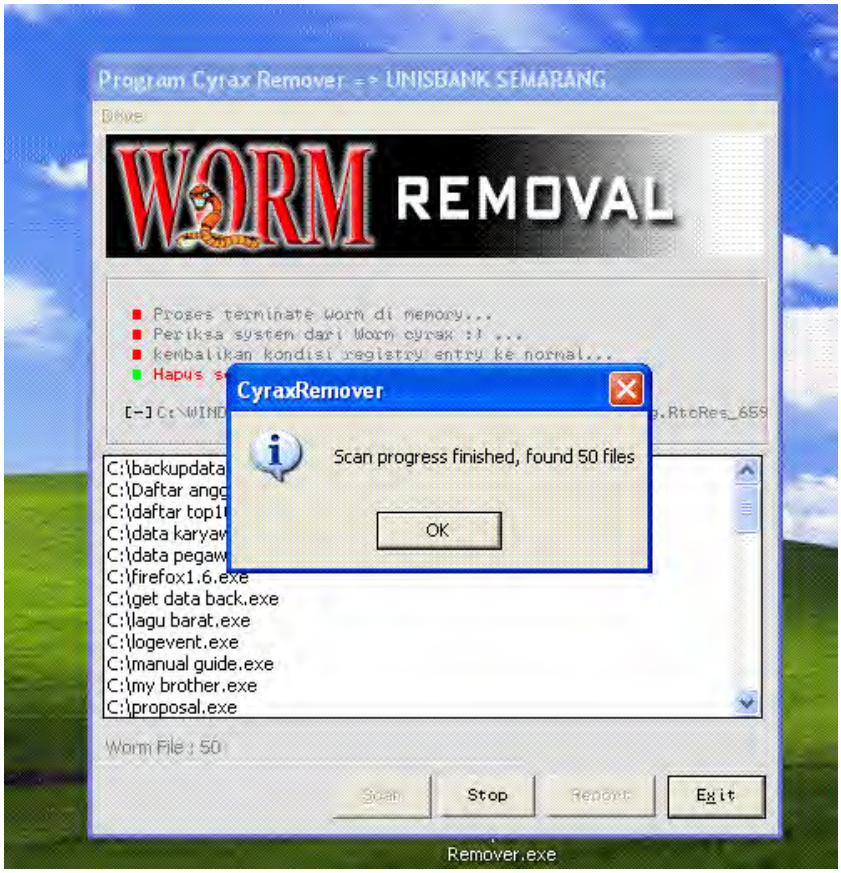
registry entry tersebut merupakan salah satu dari berbagai dampak yang diakibatkan oleh worm cyrax. Apabila ternyata worm tidak aktif dalam memori komputer maka program akan melakukan proses pencarian file – file dropper dari worm, menghapusnya bila ditemukan dan melakukan pengecekan terhadap registry.



Gambar. 4.6. Proses scanning program Cyrax Remover

c. Hasil dari proses scanning program

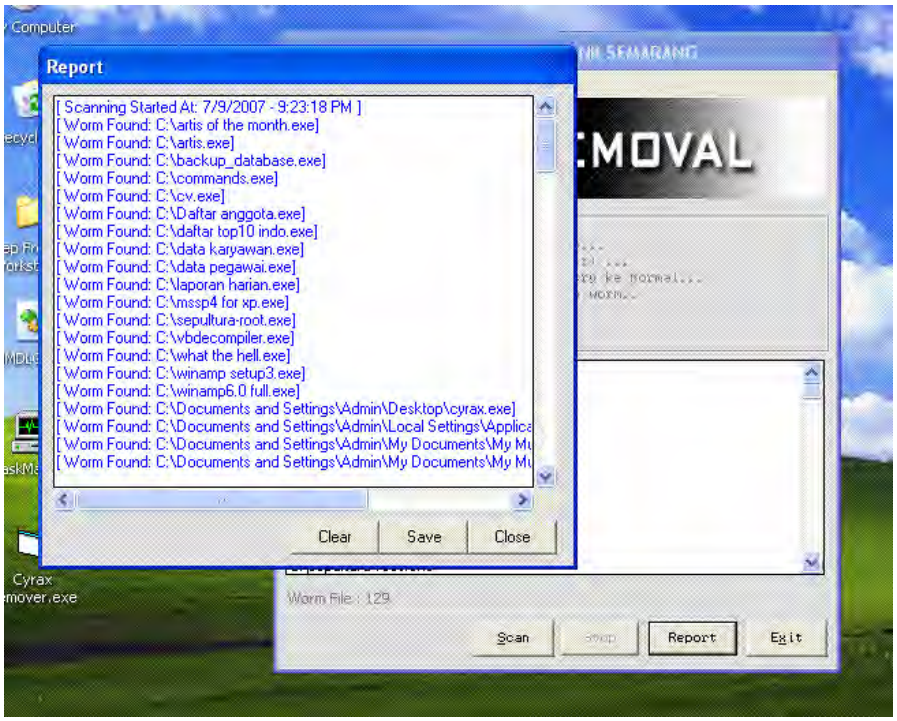
Pada tahap ini terlihat hasil dari proses scanning, yaitu ditemukannya file file droper dari worm Cyrax tersebut. Program akan secara otomatis melakukan penghapusan terhadap file worm yang telah ditemukan .



Gambar 4.7. Hasil scanning program

d. Report Program

Berikut adalah tampilan laporan dari program removal yang dapat disimpan dalam file teks atau dihapus. Laporan tersebut berisi data tentang waktu mulai proses scanning, file worm yang ditemukan dan waktu selesai proses scanning



Gambar 4.8. Tampilan Report

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari analisa dan implementasi yang telah dilakukan ada beberapa kesimpulan sebagai berikut :

a. Metode kerja worm cyrax yaitu worm yang aktif akan membuat file induk worm denagn nama “smhost.exe” dan “servlogon.exe”. dan file tersebut adalah file induk worm yang salah satunya akan aktif pada saat windows start-up. Worm akan selalu aktif pada saat pertama kali windows melakukan *start-up* apabila telah dibuat registry entry. Dan selanjutnya dilakukan monitoring windows explorer serta membuat file dropper pada setiap folder atau direktori yang dibuka dengan random filename dan random icon. Worm menggunakan aplikasi windows explorer sebagai media untuk melakukan penyebaran file dropper dari worm.
b. Dalam pengujian program yang dibuat ternyata telah dapat mengatasi dan menanggulangi dampak dari worm Cyrax pada komputer PC dan jaringan.

5.2 SARAN

Disadari sistem ini masih banyak kekurangan dan kelemahan, oleh karena itu untuk pengembangan selanjutnya disarankan :

1. Aplikisi Program Removal menggunakan teknologi proses scanning yang lebih canggih seperti CRC scanning dan program dapat di update sehingga dapat mengatasi kemungkinan adanya varian baru dari worm cyrax.
2. Dengan tampilan yang kurang menarik dan perbendaharaan data yang masih sedikit maka masih sangat perlu penyempurnaan selanjutnya.
3. Perlunya pengembangan aplikasi tersebut tidak hanya pada perangkat komputer PC atau jaringan, namun juga pada jenis perangkat mobile, seperti Ipad aau Iphone yang saat ini banyak dimanfaatkan oleh sebagian besar orang.

DAFTAR PUSTAKA

Achmad Darmal (2006), *Computer Worm 1 Secret of Underground Coding*, Jakarta, Jasakom.

Achmad Darmal (2006), *Computer Worm 2 Secret of Underground Coding*, Jakarta, Jasakom.

Aji Supriyanto (2005), *Pengantar Teknologi Informasi*, Jakarta, Salemba Infotek.

Aji Supriyanto (2009), Rancang Bangun Keamanan Dokumen Kedinasan Elektronik Berbasis XML Menggunakan Kunci Publik, Penelitian Dosen Muda (DIKTI)

Dwi Nugroho, Aji Supriyanto (2008), Analisis Sistem Kerja Virus Jenis Virus Cyrax dan teknik pengendaliannya dengan model heuristik, Unisbank, Semarang

Heribertus Yulianton, 2008, Model Data Mining Untuk Dunia Bisnis, Unisbank, Semarang

Melwin Syafrizal, (2007), Standar Sistem Manajemen Keamanan Informasi

Tri Amperiyanto (2007), *Membuat dan Membasmi Worm-Virus*, Jakarta, Elex Media Komputindo.

Wardana (2006), *Pemrograman Virus dan Spyware*, Jakarta, Jasakom.

http://computer-security-system.blogspot.com/, diakses, 10 Maret 2010

http://ekofiles.darmajaya.ac.id/index.php/info-terbaru/58-symantec , *2009, Deliusno*, Daftar Ancaman Kejahatan Komputer di Tahun 2009

http://id.wikipedia.org/wiki/Virus_komputer ,diakses, 10 maret 2010

http://id.wikipedia.org/wiki/Virus_ponsel, 2007, Dian, Dhistira. Edisi Revisi Virus Telepon Selular dan Pencegahannya.

http://research.indocisc.com/ , 2006, Teknologi Tinggi Tidak Menjamin Keamanan Informasi

http://victorx.4mg.com/VirusABC.htm , diakses 10 maret 2010

http://www.forum-bonecommunity.com/, 2009, Virus ponsel Sudah Menjadi Ancaman Nyata

Lampiran-lampiran

Lampiran-1. Data Peneliti

1. Ketua Peneliti:

Nama	:	Heribertus Yulianton, S.Si, M.Cs
NIP/NIK	:	YS.2.98.11.015
Tempat dan Tanggal Lahir	:	Rembang, 16 Juni 1973
Jenis Kelamin	:	Laki-laki
Status Perkawinan	:	Belum Kawin
Agama	:	Islam
Golongan / Pangkat	:	III-b / Penata
Jabatan Akademik	:	Asisten Ahli
Waktu Penelitian		15 Jam /minggu

2. Anggota Peneliti :

Nama	:	Arief Jananto, S.Kom, M.Cs
NIP/NIK	:	YS.2.97.03.006
Tempat dan Tanggal Lahir	:	Pemalang, 06 Januari 1974
Jenis Kelamin	:	Laki-laki
Status Perkawinan	:	Kawin
Agama	:	Islam
Golongan / Pangkat	:	III-C / Penata
Jabatan Akademik	:	Lektor
Waktu Penelitian		10 Jam / Minggu

3. Anggota Peneliti:

Nama	:	R.Soelistijadi, S.Sos, M.Kom
NIP/NIK	:	YS.2.03.07.063
Tempat dan Tanggal Lahir	:	30 Desember1966
Jenis Kelamin	:	Laki-laki
Status Perkawinan	:	Kawin
Agama	:	Islam
Golongan / Pangkat	:	III-B / Penata
Jabatan Akademik	:	Asisten Ahli
Waktu Penelitian		10 Jam / Minggu

Lampiran-2. Surat Tugas Penelitian

Lampiran-3. Realiasasi Jadwal Penelitian

Realisasi jadwal Penelitian Tahun I adalah sebagai berikut :

No	Kegiatan	Bulan ke-									
		1	2	3	4	5	6	7	8	9	10
1	Studi Pustaka dan menyusun kuisioner pra servey										
2	Survey, desk analisis, FGD Pramodel										
3	Desain DFD, ER-D, HIPO										
4	Coding Program dan Sistem Database										
5	Publikasi karya ilmiah										
6	Pelaporan kegiatan penelitian tahun I.										

UNIVERSITAS STIKUBANK SEMARANG
LEMBAGA PENELITIAN DAN PENGABDIAN MASYARAKAT (LPPM)

SEKRETARIAT :
Kampus Mugas : Jl. Tri Lomba Juang No. 1 Semarang 50241
Telp. (024) 8451976, 8311668, 8454746 Fax (024) 8443240 E-mail : LPPM@unisbank.ac.id

Kampus Bendan : Jl. Kendeng V Bendan Ngisor Semarang
Telp. (024) 8414970, Fax (024) 8441738 E-mail : lppm@unisbank.ac.id

SURAT TUGAS

Nomor : 0047/J.09/Unisbank/Pn/IV/2012

Ketua Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Stikubank (Unisbank) Semarang dengan ini memberikan tugas kepada Saudara tersebut di bawah ini:

1. N a m a : Heribertus Yulianton, S.Si, M.Cs
   NIP : YS.2.98.11.015
   Pangkat / Gol. : Penata Muda Tingkat I / III B
   Jabatan Fungsional : Asisten Ahli
2. N a m a : Arief Jananto, S.Kom, M.Cs
   NIY : YS.2.97.03.006
   Pangkat / Gol. : Penata / III
   Jabatan Akademik : Lektor
3. N a m a : R. Soelistijadi, S.Sos, M.Kom
   NIY : YU.2.03.07.063
   Pangkat / Gol. : Penata Muda Tk. I / III-B
   Jabatan Akademik : Asisten Ahli

Untuk melaksanakan Penelitian dengan judul : REKAYASA SOFTWARE ANTIVIRUS JENIS WORM SEBAGAI ALTERNATIF SOLUSI PENANGGULANGAN SERANGAN VIRUS WORM KOMPUTER dengan biaya sebesar Rp. 29.707.500,- (Dua puluh sembilan juta tujuh ratus tujuh ribu lima ratus rupiah) yang berasal dari Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 (Desentralisasi), Koordinasi Perguruan Tinggi Swasta Wilayah VI Kementerian Pendidikan dan Kebudayaan Republik Indonesia sesuai dengan surat perjanjian Pelaksanaan Penugasan Penelitian Multi Tahun, Tahun Anggaran 2012 (No. :023/O06.2/PP/SP / 2012 tanggal 24 Februari 2012.

A. Tahap Pencairan Dana:

1. Pembayaran tahap pertama sebesar 70% (tujuh puluh persen) dari jumlah biaya Penelitian yang disetujui dan dilakukan setelah dana diterima oleh Universitas Stikubank (Unisbank) Semarang melalui Pembantu Rektor II.
2. Pembayaran tahap kedua sebesar 30% dan dibayarkan setelah Peneliti mengirim kan Laporan Kemajuan Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 dan Salinan Laporan Penggunaan Keuangan 70% yang telah dilaksanakan, diserahkan paling lambat tanggal 13 Agustus 2012 kepada Kopertis Wilayah VI Jawa Tengah untuk selanjutnya diteruskan ke Dit. Litabmas Ditjen Dikti melalui LPPM Universitas Stikubank Semarang.

B. Kewajiban Peneliti:

1. Menyerahkan Laporan Kemajuan Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 sebanyak 2 (dua) eksemplar hardcopy + 1 (satu) buah CD softcopy dalam format "pdf" dan Salinan Laporan Penggunaan Keuangan 70% sebanyak 2 (dua) eksemplar hardcopy disertai Berita Acara Serah Terima Laporan Kemajuan Pelaksanaan Penelitian Multi Tahun Tahun Anggaran 2012 yang telah dilaksanakan diserahkan paling lambat tanggal 13 Agustus 2012 kepada Kopertis Wilayah VI Jawa Tengah untuk selanjutnya diteruskan ke Dit. Litabmas Ditjen Dikti melalui LPPM Universitas Stikubank Semarang.

2. Menyerahkan Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 sebanyak 8 (delapan) eksemplar hardcopy, Artikel sebanyak 2 (dua) eksemplar hardcopy, CD softcopy sebanyak 2 (dua) buah yang berisikan (Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 serta Artikel dalam format "pdf") dan Salinan Laporan Penggunaan Keuangan 100% sebanyak 2 (dua) eksemplar hardcopy disertai Berita Acara Serah Terima Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 dan Laporan Penggunaan Keuangan 100% yang telah dilaksanakan diserahkan paling lambat tanggal 14 Nopember 2012 kepada Kopertis Wilayah VI Jawa Tengah untuk selanjutnya diteruskan ke Dit.Litabmas Ditjen Dikti melalui LPPM Universitas Stikubank Semarang.
3. Segala sesuatu yang berkaitan dengan pajak menjadi tanggung jawab Peneliti dan harus disetor ke Kas Negara sesuai dengan ketentuan perundang-undangan yang berlaku.
4. Apabila ada sisa dana yang tidak dibelanjakan, Pelaksana Penelitian wajib mengembalikan ke Kas Negara.

C. Pelaporan

1. Laporan Kemajuan Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 sebanyak 2 (dua) eksemplar hardcopy + 1 (satu) buah CD softcopy dalam format "pdf" dan Salinan Laporan Penggunaan Keuangan 70% sebanyak 2 (dua) eksemplar hardcopy disertai Berita Acara Serah Terima Laporan Kemajuan Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 serta Laporan Penggunaan Keuangan 70% yang telah dilaksanakan diserahkan paling lambat tanggal 13 Agustus 2012 kepada kepada Kopertis Wilayah VI Jawa Tengah untuk selanjutnya diteruskan ke Dit. Litabmas Ditjen Dikti melalui LPPM Universitas Stikubank Semarang.

2. Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 dibuat sesuai dengan Buku Panduan Penelitian Edisi VIII Tahun 2012 dari Direktorat Penelitian dan Pengabdian kepada Masyarakat Direktorat Jenderal Pendidikan Tinggi Kementerian Pendidikan dan Kebudayaan dengan ketentuan sebagai berikut :

   a. Laporan Akhir Pelaksanaan Penelitian dalam bentuk *hardcopy* sebanyak 8 (delapan) eksemplar, dan artikel sebanyak 2 (dua) eksemplar.
   b. Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 dalam bentuk *softcopy* (CD dalam format "pdf") sebanyak 2 (dua) buah yang berisikan (Laporan Akhir Pelaksanaan Penelitian Multi Tahun,Tahun Anggaran 2012 dan Artikel).
   c. Laporan Akhir Penggunaan Keuangan 100% dalam bentuk *hardcopy* sebanyak 2 (dua) eksemplar disertai Berita Acara Serah Terima Laporan Pelaksanaan Penelitian Multi Tahun,Tahun Anggaran 2012 dan Laporan Penggunaan Keuangan 100%.
   d. Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 dalam bentuk hardcopy maunpun Softcopy diserahkan paling lambat tanggal 14 Nopemoer 2012 di LPPM (pada Jam Kerja).
   e. Bentuk ukuran kertas kuarto.
   f. Warna cover (disesuaikan dengan ketentuan yang ditetapkan)
   g. Judul penelitian pada laporan harus sesuai dengan Surat Tugas
   h. Di bawah bagian kulit ditulis: *Didanai oleh Koordinasi Perguruan Tinggi Swasta Wilayah VI, Kementerian Pendidikan dan Kebudayaan, sesuai dengan Surat Perjanjian Pelaksanaan Hibah Penelitian Nomor : 023/O05.2/ PP/SP/2012, tanggal 24 Februari 2012*

1. Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012 dalam bentuk "hard*copy*" sebanyak 8 (delapan) eksemplar, yang akan distribusikan ke :

    1. Perpustakaan Nasional Republik Indonesia 1 (satu) eksemplar
    2. Pusat Dokumentasi Ilmiah Indonesia (PDII) LIPI 1 (satu) eksemplar
    3. BAPPENAS c.q. Biro APKO 1 (satu) eksemplar
    4. DP2M Ditjend. Dikti Kemdiknas 2 (dua) eksemplar
    5. Perpustakaan Pusat Unisbank Semarang 1 (satu) eksemplar
    6. LPPM Unisabank Semarang 1 (satu) eksemplar
    7. Arsip Tim Pelaksana Penelitian 1 (satu) eksemplar

2. Sanksi
    1. Apabila sampai dengan tanggal yang telah ditetapkan, peneliti belum menyerahkan Laporan Akhir Pelaksanaan Penelitian Multi Tahun, Tahun Anggaran 2012, maka Peneliti dikenai sanksi sebagai berikut:

        b. Gugurnya hak untuk mengajukan usulan penelitian pada tahun berikutnya.

        c. Membayar denda sebesar 1% (satu permil) setiap hari dan denda maksimal 5% (lima persen) dari nilai surat Perjanjian Pelaksanaan Penelitian Multi Tahun Tahun Anggaran 2012, terhitung dari tanggal jatuh tempo yang telah ditetapkan sampai dengan berakhirnya pembayaran dana Hibah Penelitian oleh Direktorat Penelitian dan Pengabdian Kepada Masyarakat, Direktorat Jenderal Pendidikan Tinggi, Kementerian Pendidikan dan Kebudayaan melalui Kopertis Wilayah VI Jawa Tengah.

    2. Apabila di kemudian hari terbukti bahwa pada judul penelitian dijumpai adanya indikasi duplikasi dengan penelitian lain dan/atau diperoleh indikasi ketidak jujuran/itikad kurang baik yang tidak sesuai dengan kaidah ilmiah, maka kegiatan penelitian ini dinyatakan batal dan peneliti mengembalikan dana penelitian yang telah diterima ke Kas Negara.

Demikian agar dilaksanakan sebaik-baiknya.

Semarang, 13 April 2012

Mengetahui,
Rektor

Dr. Bambang Suko Priyono, MM.
NIY. Y.2.86.08.035

Ketua

Dr. Dra. Lie Liana, M.MSI
NIY. Y.2.92.07.085